ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

المكتب الوطني للمطارات
Office National Des Aéroports

DOSSIER D'APPEL D'OFFRES

Appel d'offres ouvert N° 088-24-AOO

Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Table des matières

AVIS D'APPEL D'OFFRES 1

CHAPITRE 1 : DISPOSITIONS GENERALES 3

ARTICLE 01 : OBJET DE L'APPEL D'OFFRES 3
ARTICLE 02 : MAITRE D'OUVRAGE 3
ARTICLE 03 : CONDITIONS REQUISES DES CONCURRENTS 3
ARTICLE 04 : CONTENU DU DOSSIER D'APPEL D'OFFRES 3
ARTICLE 05 : LANGUE DE L'OFFRE 4
ARTICLE 06 : DOSSIERS DES CONCURRENTS ET LISTE DES PIECES A FOURNIR 4
ARTICLE 07 : CAUTIONNEMENT PROVISOIRE 7
ARTICLE 08 : OFFRES TECHNIQUES 7
ARTICLE 09 : OFFRES COMPORTANT DES VARIANTES 7
ARTICLE 10 : OFFRE FINANCIERE 7
ARTICLE 11 : MONNAIE DE L'OFFRE 9
ARTICLE 12 : PRESENTATION DES DOSSIERS DES CONCURRENTS 9
ARTICLE 13 : DEPOT DES OFFRES DES CONCURRENTS 10
ARTICLE 14 : RETRAIT DES OFFRES DES CONCURRENTS 11
ARTICLE 15 : OUVERTURE DES PLIS ET EXAMEN ET EVALUATION DES OFFRES 12
ARTICLE 16 : CRITERES D'ADMISSIBILITE DES CONCURRENTS ET D'ATTRIBUTION DU MARCHE 12
ARTICLE 17 : RESULTATS DEFINITIFS DE L'APPEL D'OFFRES 12
ARTICLE 18 : DELAI DE VALIDITE DES OFFRES ET DELAI DE NOTIFICATION DE L'APPROBATION 13
ARTICLE 19 : ANNULATION D'UN APPEL D'OFFRES 13
ARTICLE 20 : INFORMATION, DEMANDE D'ECLAIRCISSEMENT ET RECLAMATIONS 13

CHAPITRE 2 : DISPOSITIONS PARTICULIERES 15

ANNEXE I : MODELE DE DECLARATION SUR L'HONNEUR 1
ANNEXE II : MODELE D'ACTE D'ENGAGEMENT 1
ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) –TF 3
ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) – TC 4

CAHIER DES PRESCRIPTIONS SPECIALES 5

CHAPITRE 1 : CLAUSES ADMINISTRATIVES 5

ARTICLE 01 : OBJET DU MARCHE 5
ARTICLE 02 : MODE DE PASSATION DU MARCHE 5
ARTICLE 03 : TYPE DU MARCHE 5
ARTICLE 04 : DECOMPOSITION EN TRANCHES 5
ARTICLE 05 : INDEMNITES 5
ARTICLE 06 : PIECES CONSTITUTIVES DU MARCHE 5
ARTICLE 07 : CONNAISSANCE DU DOSSIER 6
ARTICLE 08 : REFERENCES AUX TEXTES GENERAUX 6
ARTICLE 09 : RESILIATION 6
ARTICLE 10 : DOMICILE DU PRESTATAIRE 7
ARTICLE 11 : REGLEMENT DES DIFFERENDS 7
ARTICLE 12 : CAS DE FORCE MAJEURE 7
ARTICLE 13 : ENTREE EN VIGUEUR ET APPROBATION 7
ARTICLE 14 : NANTISSEMENT 7

ARTICLE 15 : FORMALITE D'ENREGISTREMENT 8
ARTICLE 16 : DROIT APPLICABLE 8
ARTICLE 17 : DROITS ET TAXES 8

CHAPITRE 2 : CLAUSES TECHNIQUES –Tranche ferme – ____ 10

ARTICLE 01 : MAITRE D'ŒUVRE 10
ARTICLE 02 : GARANTIE PARTICULIAIRE 10
ARTICLE 03 : NATURE DES PRESTATIONS ET REVISION DES PRIX 10
ARTICLE 04 : DELAI D'EXECUTION 10
ARTICLE 05 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE 10
ARTICLE 06 : DELAI DE GARANTIE 11
ARTICLE 07 : RECEPTION DES PRESTATIONS 11
ARTICLE 08 : MODE DE PAIEMENT 11
ARTICLE 09 : PENALITES POUR RETARD 12
ARTICLE 10 : BREVETS 12
ARTICLE 11 : LOIS ET NORMES 12
ARTICLE 12 : CONSISTANCE DES PRESTATIONS 13
ARTICLE 13 : CONTROLE ET VERIFICATION 38
ARTICLE 14 : DEFINITION DES PRIX 38

CHAPITRE 3 : CLAUSES TECHNIQUES – Tranche conditionnelle- ____ 39

ARTICLE 01 : MAITRE D'ŒUVRE 39
ARTICLE 02 : NATURE DES PRESTATIONS ET REVISION DES PRIX 39
ARTICLE 03 : DUREE DU MARCHE 39
ARTICLE 04 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE - TRANCHE CONDITIONNELLE . 39
ARTICLE 05 : DELAI DE GARANTIE 39
ARTICLE 06 : RECEPTION DES PRESTATIONS DE TRANCHE CONDITIONNELLE 39
ARTICLE 07 : MODE DE PAIEMENT 40
ARTICLE 08 : PENALITES POUR RETARD 40
ARTICLE 09 : BREVETS 40
ARTICLE 10 : NORMES 40
ARTICLE 11 : GARANTIE PARTICULIERE 40
ARTICLE 12 : DESCRIPTION TECHNIQUE DES PRESTATIONS 41
ARTICLE 13 : CONTROLE ET VERIFICATION 42
ARTICLE 14 : DEFINITION DES PRIX 43

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

AVIS D'APPEL D'OFFRES

OUVERT SUR "OFFRES DE PRIX"

N°088-24-AOO

Le **jeudi 11 juillet 2024** à **10 heures**, il sera procédé, dans la salle de la Commission d'Appels d'Offres située au bâtiment de la Direction des Achats et de la Logistique (près de l'Aéroport CASABLANCA Mohammed V) à l'ouverture des plis relatifs à l'appel d'offres **sur offres de prix** concernant : **Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information.**

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Le dossier d'appel d'offres peut être retiré **gratuitement**, auprès de la cellule Interface Achats au Département des Achats situé au bâtiment de la Direction des Achats et de la Logistique (près de l'Aéroport CASABLANCA Mohammed V). Il peut également être téléchargé à partir du portail des marchés publics **www.marchespublics.gov.ma** et **à titre indicatif** à partir de l'adresse électronique **www.onda.ma.**

Le cautionnement provisoire est fixé à la somme de : **249 000,00 DH.**

La constitution du cautionnement provisoire doit être effectuée **exclusivement par voie électronique via le portail des marchés publics**, dans les conditions fixées par l'arrêté n° 1692-23 du 4 hija 1444 (23 juin 2023) mentionné ci-dessous.

L'estimation des coûts des prestations établie par le maitre d'ouvrage est fixée à la somme TVA comprise de :

- **Tranche ferme : 14 004 000,00 DH**
- **Tranche conditionnelle : 2 640 000,00 DH/AN**

Le contenu, la présentation ainsi que le dépôt des dossiers des concurrents doivent être conformes aux dispositions des articles 06, 07, 08, 09, 10, 11, 12, 13 et 14 du règlement de la consultation du présent appel d'offres.

En effet, le dépôt et le retrait des plis et des offres des concurrents s'effectuent pour le présent appel d'offres, **obligatoirement**, **par voie électronique,** via le portail des marchés publics, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatives aux marchés publics.

Les plis déposés, transmis ou reçus sur support papier ou postérieurement au jour et à l'heure fixés ci-dessus ne sont pas admis.

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

REGLEMENT DE CONSULTATION

Appel d'offres ouvert N° 088-24-AOO

Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

TABLE DES MATIERES

CHAPITRE 1 : DISPOSITIONS GENERALES 3

ARTICLE 01 : OBJET DE L'APPEL D'OFFRES 3
ARTICLE 02 : MAITRE D'OUVRAGE....3
ARTICLE 03 : CONDITIONS REQUISES DES CONCURRENTS 3
ARTICLE 04 : CONTENU DU DOSSIER D'APPEL D'OFFRES 3
ARTICLE 05 : LANGUE DE L'OFFRE 4
ARTICLE 06 : DOSSIERS DES CONCURRENTS ET LISTE DES PIECES A FOURNIR 4
ARTICLE 07 : CAUTIONNEMENT PROVISOIRE 7
ARTICLE 08 : OFFRES TECHNIQUES 7
ARTICLE 09 : OFFRES COMPORTANT DES VARIANTES 7
ARTICLE 10 : OFFRE FINANCIERE 7
ARTICLE 11 : MONNAIE DE L'OFFRE 9
ARTICLE 12 : PRESENTATION DES DOSSIERS DES CONCURRENTS 9
ARTICLE 13 : DEPOT DES OFFRES DES CONCURRENTS 10
ARTICLE 14 : RETRAIT DES OFFRES DES CONCURRENTS 11
ARTICLE 15 : OUVERTURE DES PLIS ET EXAMEN ET EVALUATION DES OFFRES 12
ARTICLE 16 : CRITERES D'ADMISSIBILITE DES CONCURRENTS ET D'ATTRIBUTION DU MARCHE 12
ARTICLE 17 : RESULTATS DEFINITIFS DE L'APPEL D'OFFRES 12
ARTICLE 18 : DELAI DE VALIDITE DES OFFRES ET DELAI DE NOTIFICATION DE L'APPROBATION 13
ARTICLE 19 : ANNULATION D'UN APPEL D'OFFRES 13
ARTICLE 20 : INFORMATION, DEMANDE D'ECLAIRCISSEMENT ET RECLAMATIONS 13

CHAPITRE 2 : DISPOSITIONS PARTICULIERES 15

ANNEXE I : MODELE DE DECLARATION SUR L'HONNEUR 1
ANNEXE II : MODELE D'ACTE D'ENGAGEMENT 1
ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) –TF 3
ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) – TC 4

CHAPITRE 1 : DISPOSITIONS GENERALES

ARTICLE 01 : OBJET DE L'APPEL D'OFFRES

Le présent règlement concerne la consultation relative au projet : **Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information.**

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

ARTICLE 02 : MAITRE D'OUVRAGE

Le maître d'ouvrage est l'Office National des Aéroports (ONDA).

ARTICLE 03 : CONDITIONS REQUISES DES CONCURRENTS

Peuvent valablement participer et être attributaires des marchés publics de l'ONDA, dans le cadre des procédures prévues par le présent règlement de consultation, les personnes physiques ou morales qui répondent aux conditions de l'article 24 du règlement des marchés de l'ONDA en vigueur.

ARTICLE 04 : CONTENU DU DOSSIER D'APPEL D'OFFRES

Le dossier d'appel d'offres comprend :

01. L'avis d'appel d'offres ;
02. Le présent règlement de consultation ;
03. Le cahier des prescriptions spéciales (CPS) ;
04. Le modèle d'acte d'engagement ;
05. Le modèle de la déclaration sur l'honneur ;
06. Le modèle du bordereau des prix-détails estimatifs ;
07. Le modèle du bordereau des prix pour approvisionnements, le cas échéant ;
08. Le modèle du sous détail des prix, le cas échéant ;
09. Tout autre modèle joint au présent dossier d'appel d'offres ;
10. Les plans et documents techniques, le cas échéant.
11. Le règlement relatif aux marchés publics de l'Office National des Aéroports, approuvé le 09 juillet 2014, téléchargeable sur le site de l'ONDA à l'adresse suivante :

    http://www.onda.ma/Je-suis-Professionnel/Appels-d'offres/Règlementation-des-marchés-de-l'ONDA ;

NB : Tout concurrent est tenu de prendre connaissance et d'examiner toutes les instructions, modèles et spécifications contenues dans les documents de la consultation.

Le concurrent assumera les risques de défaut de fourniture des renseignements exigés par les documents de la consultation ou de la présentation d'une offre non conforme, au regard, des exigences des documents de la consultation. Ces carences peuvent entraîner

le rejet de son offre.

ARTICLE 05 : LANGUE DE L'OFFRE

L'offre préparée par le concurrent ainsi que toute correspondance et tout document concernant l'offre échangés entre le concurrent et l'ONDA doivent être rédigés en **LANGUE FRANÇAISE**.

Tout document imprimé fourni par le candidat peut être rédigé en une autre langue dès lors qu'il est accompagné d'une traduction en langue française par une personne/autorité compétente (Les documents en arabe ne nécessite pas de traduction en français), des passages intéressants l'offre. Dans ce cas et aux fins de l'interprétation de l'offre, la traduction française fait foi.

Seules les offres techniques peuvent être fournies en langue **ARABE ou ANGLAISE**. Toutefois, en cas de besoin la Commission des Appels d'Offres peut demander, au concurrent et aux frais de ce dernier, la traduction des documents constituant l'offre technique en langue française.

ARTICLE 06 : DOSSIERS DES CONCURRENTS ET LISTE DES PIECES A FOURNIR

Conformément aux articles 25, 27, 28, 29 et 30 du règlement des marchés de l'ONDA en vigueur, chaque concurrent est tenu de présenter les pièces suivantes :

A. Le dossier administratif : Pièces exigées

Pour chaque concurrent, au moment de la présentation des offres :

A1. **Une déclaration sur l'honneur**, en un exemplaire unique, conformément au modèle joint au présent règlement de consultation ;

A2. Le **cautionnement provisoire**, tel que précisé au niveau de l'avis d'appel d'offres et dans les conditions fixées par l'article 7 ci-dessous.

A3. Pour les groupements, en plus des pièces citées ci-dessus, une copie légalisée de la **convention constitutive du groupement** prévue à l'article 140 du règlement des marchés de l'ONDA en vigueur.

La signature portée par chaque membre du groupement doit être originale et légalisée par une personne/autorité compétente. De ce fait, toute convention de groupement portant une signature scannée sera rejetée.

Pour les établissements publics :

A1. **Une déclaration sur l'honneur**, en un exemplaire unique, conformément au modèle joint au présent règlement de consultation.

A2. Le **cautionnement provisoire**, tel que précisé au niveau de l'avis d'appel d'offres et dans les conditions fixées par l'article 7 ci-dessous.

A3. Pour les groupements, en plus des pièces citées ci-dessus, une copie légalisée de la **convention constitutive du groupement** prévue à l'article 140 du règlement des marchés de l'ONDA en vigueur.

La signature portée par chaque membre du groupement doit être originale et légalisée par une personne/autorité compétente. De ce fait, toute convention de groupement portant une signature scannée sera rejetée.

A4. **Une copie du texte** l'habilitant à exécuter les prestations objet du marché.

B. Le complément du dossier administratif : Pièces exigées

Pour le concurrent auquel il est envisagé d'attribuer le marché, dans les conditions fixées à l'article 40 du règlement des marchés de l'ONDA en vigueur :

B1. **Les pièces justifiant les pouvoirs** conférés à la personne agissant au nom du concurrent. Ces pièces varient selon la forme juridique du concurrent :

- S'il s'agit d'une **personne physique** agissant pour son propre compte :
  - Aucune pièce n'est exigée ;
- S'il s'agit d'un **représentant**, celui-ci doit présenter selon le cas :
  - Une copie conforme de la procuration **légalisée** lorsqu'il agit au nom d'une personne physique ;
  - Un extrait des statuts de la société et/ou le procès-verbal de l'organe compétent lui donnant pouvoir selon la forme juridique de la société, lorsqu'il agit au nom d'une personne morale ;
  - L'acte par lequel la personne habilitée délègue son pouvoir à une tierce personne, le cas échéant.

B2. **Une attestation fiscale** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties prévues à l'article 24 du **règlement des marchés de l'ONDA en vigueur**.

Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé.

NB : Pour les concurrents installés au Maroc, le document « Demande d'attestation de régularité fiscale » délivré par la Direction Générale des Impôts n'est pas acceptable. Seule l'attestation fiscale pour concurrents aux marchés publics délivrée par la Trésorerie Générale du Royaume est acceptable.

B3. **Une attestation** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse Nationale de Sécurité Sociale (**CNSS**) certifiant que le concurrent est en situation régulière envers cet organisme ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme.

NB : La validité des pièces prévus aux B2) et B3) ci-dessus est appréciée sur la base de leur date de production par rapport de la date du dépôt du complément administratif (cf. paragraphe 5 de l'article 40 du règlement des marchés de l'ONDA).

B4. Le certificat d'immatriculation au **registre de commerce** pour les personnes assujetties à l'obligation d'immatriculation conformément à la législation en vigueur;

NB : **Pour les concurrents non installés au Maroc** l'équivalent des attestations visées aux paragraphes **B2**, **B3** et **B4** ci-dessus, délivrées par les administrations ou les organismes compétents de leurs pays d'origine ou de provenance.

A défaut de la délivrance de tels documents par les administrations ou les organismes compétents de leur pays d'origine ou de provenance, lesdites attestations peuvent être remplacées par une attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.

Pour les établissements publics :

B1. **Une attestation fiscale** ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant qu'il est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties prévues à l'article 24 du règlement des marchés de l'ONDA en vigueur. Cette attestation, qui n'est exigée que pour les organismes soumis au régime de la fiscalité, doit mentionner l'activité au titre de laquelle le concurrent est imposé ;

NB : Pour les concurrents installés au Maroc, le document « Demande d'attestation de régularité fiscale » délivré par la Direction Générale des Impôts n'est pas acceptable. Seule l'attestation fiscale pour concurrents aux marchés publics délivrée par la Trésorerie Générale du Royaume est acceptable.

B2. **Une attestation** ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse nationale de Sécurité Sociale (**CNSS**) certifiant que le concurrent est en situation régulière envers cet organisme conformément aux dispositions prévues à cet effet à l'article 24 ci-dessus ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 Joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme.

NB : La validité des pièces prévues aux **B1** et **B2** ci-dessus est appréciée sur la base de leur date de production par rapport de la date du dépôt du complément administratif (cf. paragraphe 5 de l'article 40 du règlement des marchés de l'ONDA).

C. Le dossier technique :

Chaque concurrent est tenu de présenter un dossier technique composé des pièces détaillées dans les dispositions particulières ci-dessous (chapitre 2 du présent règlement de consultation).

Lorsqu'il est prévu, au niveau des dispositions particulières (chapitre 2 du présent règlement de consultation), la présentation d'un certificat de qualification et de classification ou d'un certificat d'agrément. Ledit certificat tient lieu du dossier technique.

Pour les groupements, il y a lieu de se conformer aux dispositions de l'article 140 du règlement des marchés de l'ONDA en vigueur relatives au dossier technique.

D. Le dossier additif :

Il comprend toutes pièces complémentaires exigées par le présent règlement de consultation tel que détaillé dans les dispositions particulières (chapitre 2 du présent règlement de consultation).

E. Le cahier des prescriptions spéciales :

Paraphé et signé, en toutes les pages et sans réserves, par le concurrent ou la personne habilitée par lui à cet effet.

ARTICLE 07 : CAUTIONNEMENT PROVISOIRE

Chaque concurrent est tenu de produire un cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu, tel qu'indiqué sur l'avis d'appel d'offres.

Le récépissé du cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu **doivent être émis par un organisme Marocain agréé et arrêtés en Dirhams Marocains (MAD).**

NB 1 : Etant donné que la soumission par voie électronique est obligatoire, **la constitution du cautionnement provisoire s'effectue exclusivement par voie électronique, via le portail des marchés publics**, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics et conformément aux conditions d'utilisation dudit portail.

NB 2 : Le cautionnement ne doit pas être limité dans le temps, ni comporter des conditions et/ou réserves de la part de la banque et/ou du soumissionnaire.

NB 3 : En cas de groupement, le cautionnement provisoire doit être souscrit conformément aux conditions d'utilisation du portail des marchés publics.

Aussi, **le récépissé du cautionnement provisoire** ou **l'attestation de la caution personnelle et solidaire** en tenant lieu **doivent préciser la mention suivante :**

« Le présent cautionnement est délivré dans le cadre d'un groupement et, en cas de défaillance, le montant dudit cautionnement reste acquis au maître d'ouvrage abstraction faite du membre défaillant ».

Le cautionnement provisoire reste acquis à l'ONDA dans les cas prévus par :

- L'article 15 du CCAG EMO ;
- L'article 18 du CCAG Travaux ;
- L'article 40 du règlement des marchés publics de l'ONDA.

ARTICLE 08 : OFFRES TECHNIQUES

Lorsque la présentation d'une offre technique est exigée conformément à l'article 28 du règlement des marchés de l'ONDA, les concurrents doivent fournir les pièces détaillées dans les dispositions particulières **(cf. chapitre 2 du présent règlement de la consultation)**.

ARTICLE 09 : OFFRES COMPORTANT DES VARIANTES

Les offres variantes ne sont pas prévues pour le présent appel d'offres.

ARTICLE 10 : OFFRE FINANCIERE

L'offre financière comprend :

1. **L'acte d'engagement,** conformément à **l'ANNEXE II,** en un seul exemplaire.

Cet acte d'engagement doit être dûment rempli, et comportant **le relevé d'identité bancaire (RIB)**, est signé par le concurrent ou son représentant habilité, sans qu'un même représentant puisse représenter plus d'un concurrent à la fois pour le même appel d'offres.

Lorsque l'acte d'engagement est souscrit par un groupement tel qu'il est défini à l'article 140 du règlement des marchés publics de l'ONDA, il doit être signé soit par chacun des membres du groupement ; soit seulement par le mandataire si celui-ci justifie des

habilitations sous forme de **procurations légalisées** pour représenter les membres du groupement lors de la procédure de passation du marché.

Cette dernière disposition est applicable également **s'il s'agit d'un appel d'offres alloti** dont le règlement de consultation prévoit un acte d'engagement pour chaque lot ; Abstraction faite de la répartition des lots entre les membres du groupement, qu'il soit conjoint ou solidaire.

Si le groupement est conjoint, il doit présenter un acte d'engagement unique qui indique le montant total du marché et **doit préciser** la ou les parties des prestations que chacun des membres du groupement conjoint s'engage à réaliser.

Si le groupement est solidaire, il doit présenter un acte d'engagement unique qui indique le montant total du marché et l'ensemble des prestations que les membres du groupement s'engagent solidairement à réaliser, cet acte d'engagement **peut**, le cas échéant, indiquer les prestations que chacun des membres s'engage à réaliser dans le cadre dudit marché

NB : Le montant total de l'acte d'engagement doit être libellé en **chiffres** et en toutes **lettres**.

2. **Le bordereau des prix-détail estimatif**, conformément à l'**ANNEXE III**. Les concurrents **ne doivent** pas proposer plusieurs prix en monnaies différentes pour une même ligne figurant au niveau du bordereau des prix-détail estimatif.

Conformément à l'article 27 du règlement des marchés de l'ONDA en vigueur :

- Les prix unitaires du bordereau des prix, du détail estimatif et ceux du bordereau des prix-détail estimatif et les prix forfaitaires du bordereau du prix global et de la décomposition du montant global **doivent être libellés en chiffres**.
- En cas de discordance entre les prix unitaires du bordereau des prix et ceux du détail estimatif, les prix du bordereau des prix prévalent.
- En cas de discordance entre les montants totaux du bordereau du prix global et ceux de la décomposition du montant global, le montant total la décomposition du montant global prévaut.
- Les montants totaux du bordereau des prix-détail estimatif, du bordereau du prix global et de la décomposition du montant global **doivent être libellés en chiffres.**
- En cas de discordance entre le montant total de l'acte d'engagement, et de celui du détail estimatif, du bordereau des prix-détail estimatif ou du bordereau du prix global, selon le cas, le montant de ces derniers documents est tenu pour bons pour établir le montant réel de l'acte d'engagement.

3. **Le sous détail des prix**, le cas échéant.
4. **Le bordereau des prix pour approvisionnements**, lorsqu'il est prévu par le cahier de prescriptions spéciales.

NB : OFFRE FINANCIERE EXCESSIVE

Lorsque l'offre la plus avantageuse est supérieure **de plus de vingt pour cent (20%)** par rapport à l'estimation du coût des prestations établie par le maître d'ouvrage pour les **marchés de travaux**, **de fournitures** et **de services autres que ceux qui portent sur les**

études, elle est jugée **excessive** et est **systématiquement rejetée par la commission d'appel d'offres** et ce, conformément à l'article 41 du règlement des marchés de l'ONDA en vigueur.

ARTICLE 11 : MONNAIE DE L'OFFRE

Les offres financières **des concurrents résidents au Maroc** doivent être exprimées **exclusivement** en Dirhams Marocains (**MAD**). En cas de groupement avec des concurrents non-résidents au Maroc, les prix des prestations qui seront payées au membre résident au Maroc doivent être exprimés en Dirhams Marocains.

Lorsque le concurrent est non-résident au Maroc, son offre peut être exprimée strictement dans la(es) monnaie(s) suivante(s) :

- **MAD** : Dirhams marocains
- **EUR** : Euros
- **USD :** Dollars américains

Les offres exprimées en monnaies étrangères (**EUR/USD**) seront, pour les besoins d'évaluation et de comparaison, converties en Dirham. Cette conversion s'effectue sur la base du **cours de référence du dirham** en vigueur, du premier jour ouvrable de la semaine précédant celle du jour d'ouverture des plis, donné par Bank Al-Maghrib.

NB : Un concurrent **ne doit pas** proposer plusieurs prix en monnaies différentes pour une même ligne figurant au niveau du bordereau des prix-détail estimatif. **A défaut, son offre sera écartée.**

ARTICLE 12 : PRESENTATION DES DOSSIERS DES CONCURRENTS

Comme précisé dans l'avis d'appel d'offres, **la soumission par voie électronique est obligatoire.** De ce fait, il est demandé aux concurrents de présenter, **électroniquement**, les documents exigés, sous le **format standard A4** à l'exception des plans qui peuvent être présentés sous format A3.

Les pièces produites par chaque concurrent doivent être insérées, individuellement, dans l'enveloppe électronique les concernant.

Aussi, conformément aux conditions d'utilisation du portail des marchés publics, chaque document doit être signé, électroniquement, par le concurrent ou la personne dûment habilitée à le représenter, à l'exception des pièces dématérialisées.

Contenu des enveloppes :

1. Lorsque l'offre technique n'est pas exigée, **Deux (02) enveloppes** distinctes :
    a. **La première enveloppe** contient :
        1. Les pièces du **dossier administratif** (Article 6 § A) ;
        2. Les pièces du **dossier technique** (Article 6 § C) ;
        3. Les pièces du **dossier additif** (Article 6 § D), le cas échéant ;
        4. Le **c**ahier des **p**rescriptions **s**péciales (Article 6 § E).
    b. **La deuxième enveloppe** contient les pièces exigées de l'offre financière telles que détaillées dans l'article 10 ci-dessus ;
2. Lorsque l'offre technique est exigée, **Trois (03) enveloppes** distinctes :

a. **La première enveloppe** contient :
   1. Les pièces du **dossier administratif** (Article 6 § A) ;
   2. Les pièces du **dossier technique** (Article 6 § C) ;
   3. Les pièces du **dossier** additif (Article 6 § D), le cas échéant.
   4. Le **c**ahier des **p**rescriptions **s**péciales (Article 6 § E).

b. **La deuxième enveloppe** contient les pièces exigées de l'offre financière telles que détaillées dans l'article 10 ci-dessus ;

c. **La troisième enveloppe** contient les pièces exigées de l'offre technique telles que détaillées dans l'article 8 ci-dessus.

NB : Lorsque **l'appel d'offres est alloti** :

- Le concurrent peut participer à un ou plusieurs lots ;
- Le concurrent doit présenter les offres techniques, si elles sont exigées et les offres financières **séparément** pour chaque lot.

A défaut, son offre sera écartée.

ARTICLE 13 : DEPOT DES OFFRES DES CONCURRENTS

1. Dépôt des échantillons, prospectus, notices ou autres documents techniques

Lorsque le dépôt d'échantillons et/ou la présentation de prospectus, notices ou autres documents techniques est exigé, conformément à l'article 34 du règlement des marchés de l'ONDA, les concurrents doivent déposer les échantillons/documents détaillés dans les dispositions particulières (**cf. chapitre 2 du présent règlement de la consultation**), dans les conditions fixées au niveau de l'avis d'appel d'offres.

2. Dépôt des plis par voie électronique

La soumission par voie électronique est obligatoire. Par conséquent, les plis des concurrents doivent être déposés dans les conditions fixées dans l'avis d'appel d'offres du présent dossier d'appel d'offres.

En effet et sauf stipulations différentes dans l'avis d'appel d'offres, le dépôt et le retrait des plis et des offres des concurrents s'effectuent pour le présent appel d'offres, **obligatoirement**, **par voie électronique,** via le portail des marchés publics, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics.

Les plis déposés, transmis ou reçus sur support papier ou postérieurement au jour et à l'heure fixés ci-dessus ne sont pas admis.

Toutes les pièces exigées par le présent règlement de consultation, **doivent être insérées, individuellement, dans l'enveloppe électronique les concernant et ce, comme détaillé dans l'article 12 ci-dessus**.

Aussi, conformément aux conditions d'utilisation du portail des marchés publics, chaque document doit être signé, électroniquement, par le concurrent ou la personne dûment habilitée à le représenter, à l'exception des pièces dématérialisées et ce, avant leur insertion dans **l'enveloppe électronique** correspondante.

Cette signature s'effectue par le concurrent au moyen d'un certificat de signature électronique conformément aux dispositions des textes législatifs et réglementaires en vigueur et aux conditions d'utilisation du portail des marchés publics.

Les plis sont déposés moyennant le certificat de signature électronique susmentionné.

Le dépôt des plis fait l'objet d'un horodatage automatique au niveau du portail des marchés publics, mentionnant la date et l'heure de dépôt électronique et de l'envoi de l'accusé de réception électronique au concurrent concerné à travers ledit portail.

3. Dépôt des plis complémentaires

Le pli contenant les pièces produites, suite à la demande de la commission d'appel d'offres, par le concurrent auquel il est envisagé d'attribuer le marché, doit être, **selon le choix fixé** dans la demande de ladite commission :

- soit **déposé**, sur support papier, contre récépissé, dans le bureau du maître d'ouvrage indiqué dans la demande ;
- soit **envoyé**, sur support papier, par courrier recommandé avec accusé de réception, au bureau précité ;
- soit transmis, **par voie électronique**, via le portail des marchés publics, dans les conditions fixées par l'arrêté n°1692-23 du 4 hija 1444 (23 juin 2023) relatif à la dématérialisation des procédures, des documents et des pièces relatifs aux marchés publics.

Les plis déposés, transmis ou reçus postérieurement au délai fixé dans la demande de la commission **ne sont pas admis**.

NB :

La conclusion du marché issu de la procédure de la réponse électronique aux appels d'offres est effectuée sur la base d'un dossier sous format électronique.

Toutefois, l'adjudicataire est tenu de présenter sous format papier tout document demandé pour la conclusion du marché.

ARTICLE 14 : RETRAIT DES OFFRES DES CONCURRENTS

a. **Tout pli déposé électroniquement** peut être retiré par le concurrent antérieurement au jour et à l'heure fixés pour la séance d'ouverture des plis.

   Le retrait de tout pli s'effectue au moyen du **certificat de signature électronique** ayant servi au dépôt de ce pli.

   Les informations relatives au retrait des plis sont enregistrées automatiquement sur le registre de dépôts des plis.

   Les concurrents ayant retiré leurs plis peuvent présenter de nouveaux plis dans les conditions prévues par le présent règlement de consultation et avant la date et heure limites d'ouverture des plis.

b. **Les échantillons, prototypes, prospectus, notices ou autres documents techniques** déposés ou reçus peuvent être retirés au plus tard le jour ouvrable précédant le jour et l'heure fixés pour l'ouverture des plis.

Le retrait des échantillons, prototypes, prospectus, notices ou autres documents techniques fait l'objet d'une demande écrite et signée par le concurrent ou son représentant dûment habilité. La date et l'heure du retrait sont enregistrées par le maître d'ouvrage dans un registre.

Les concurrents ayant retiré leurs échantillons, prototypes, prospectus, notices ou autres documents techniques peuvent présenter de nouveaux échantillons, prototypes, prospectus, notices ou autres documents techniques dans les conditions prévues dans le présent règlement de consultation.

ARTICLE 15 : OUVERTURE DES PLIS ET EXAMEN ET EVALUATION DES OFFRES

La séance d'ouverture des plis des concurrents **est publique.** Elle se tient au lieu, au jour et à l'heure prévus par le dossier d'appel d'offres ; si ce jour est **déclaré férié ou chômé**, la réunion se tient le jour ouvrable suivant à la même heure, et ce conformément à l'article 36 paragraphe 1 du règlement des marchés de l'ONDA en vigueur.

Conformément aux conditions d'utilisation du portail des marchés publics, il est procédé à l'ouverture des plis et à l'examen des offres des concurrents déposés **par voie électronique** dans les conditions fixées, notamment, dans articles **36, 37, 38, 39, 40, 41 et 42** du règlement des marchés de l'ONDA en vigueur jusqu'à l'achèvement des travaux de la commission de la consultation.

Les résultats de l'évaluation des offres des concurrents déposées **par voie électronique** sont portés à la connaissance de ces derniers au fur et à mesure du déroulement des travaux de la commission de consultation.

Lorsqu'il s'agit d'un appel d'offres alloti, la commission procède pour l'attribution des lots à l'ouverture, l'examen des offres de chaque lot et l'attribution des lots, lot par lot, dans l'ordre de leur énumération dans le dossier d'appel d'offres.

L'adjudication d'un lot n'est pas conditionnée par l'adjudication de l'un ou des autres lots quelle que soit leur énumération dans le dossier d'appel d'offres, sauf stipulations contraires dans les dispositions particulières du présent règlement de consultation. Par conséquent, l'ouverture des plis d'un lot peut être effectuée par la commission même si le lot précédent dans l'appel d'offres n'est pas encore adjugé.

ARTICLE 16 : CRITERES D'ADMISSIBILITE DES CONCURRENTS ET D'ATTRIBUTION DU MARCHE

Les critères d'admissibilité des concurrents sont détaillés dans les dispositions particulières (chapitre 2 du présent règlement de la consultation).

ARTICLE 17 : RESULTATS DEFINITIFS DE L'APPEL D'OFFRES

Le maître d'ouvrage informe le concurrent attributaire du marché de l'acceptation de son offre **via le portail des marchés publics** ou **par lettre recommandée avec accusé de réception** ou **par tout autre moyen de communication donnant date certaine**. Cette lettre est adressée dans un délai de **cinq (05) jours ouvrables** au maximum à compter du lendemain de la date d'achèvement des travaux de la commission.

Dans le même délai, il avise également les concurrents éliminés du rejet de leurs offres, en leur indiquant les motifs de leur éviction **via le portail des marchés publics** ou par **lettre**

recommandée avec accusé de réception ou par **tout autre moyen de communication donnant date certaine**.

Les échantillons ou prototypes, le cas échéant, sont restitués, après achèvement du délai de réclamation auprès du maître d'ouvrage, aux concurrents éliminés contre décharge.

ARTICLE 18 : DELAI DE VALIDITE DES OFFRES ET DELAI DE NOTIFICATION DE L'APPROBATION

Les concurrents restent engagés par leurs offres pendant un délai de **soixante-quinze (75)** jours, à compter de la date de la séance d'ouverture des plis.

Ce délai peut être prorogé dans les conditions prévues aux articles 33 et 136 du règlement des marchés de l'ONDA en vigueur.

Toutefois, la signature du marché par l'attributaire vaut le maintien de son offre.

ARTICLE 19 : ANNULATION D'UN APPEL D'OFFRES

L'autorité compétente (ONDA) peut, sans de ce fait encourir aucune responsabilité à l'égard des concurrents et quel que soit le stade de la procédure pour la conclusion du marché, annuler l'appel d'offres. Cette annulation intervient dans les cas suivants :

1. Lorsque les données économiques ou techniques des prestations objet de l'appel d'offres ont été fondamentalement modifiées ;
2. Lorsque des circonstances exceptionnelles ne permettent pas d'assurer l'exécution normale du marché ;
3. Lorsque les offres reçues dépassent les crédits budgétaires alloués au marché ;
4. Lorsqu'un vice de procédure a été décelé ;
5. En cas de réclamation fondée d'un concurrent **sous réserve** des dispositions de l'article 152 du règlement des marchés de l'ONDA en vigueur;

En cas d'annulation d'un appel d'offres dans les conditions prévues ci-dessus, les concurrents ou l'attributaire du marché ne peuvent prétendre à indemnité.

ARTICLE 20 : INFORMATION, DEMANDE D'ECLAIRCISSEMENT ET RECLAMATIONS

Tout concurrent peut demander au maître d'ouvrage, **par courrier** porté avec accusé de réception, **par lettre recommandée** avec accusé de réception ou par **voie électronique** de lui fournir des éclaircissements ou renseignements concernant l'appel d'offres ou les documents y afférents, **exclusivement**, aux coordonnées suivantes :

	Adresse	**Département des Achats** Office National des Aéroports Aéroport Casablanca Mohammed V – Nouaceur
	Boite postale	BP 52, Aéroport Casablanca Mohammed V – Nouaceur
	E-mail	achats@onda.ma

Portail des marchés publics https://www.marchespublics.gov.ma

NB : Cette demande **n'est recevable que** si elle parvient au maître d'ouvrage au moins **sept (7) jours** avant la date prévue pour la séance d'ouverture des plis.

Les réclamations des concurrents doivent être formulées dans les conditions fixées par l'article 152 du règlement des marchés publics de l'ONDA.

En effet, les réclamations des concurrents doivent être introduites **à partir de la date de la publication** de l'avis d'appel à la concurrence et **au plus tard cinq (05) jours** après l'affichage du résultat du présent appel d'offres.

Toutefois, la réclamation du concurrent pour contester les motifs d'éviction, doit intervenir à compter de la date de réception de la lettre d'éviction et au plus tard dans les cinq (05) jours suivants.

Important : Toute correspondance émanant d'un concurrent, sur support papier ou par voie électronique, doit être signée, datée et établie sur papier en-tête précisant notamment, la dénomination/la raison sociale du concurrent ainsi que le nom, le prénom et la qualité de la personne habilitée ayant émis et signé ladite correspondance. A défaut, l'ONDA se réserve le droit de ne pas donner une suite à ladite correspondance.

CHAPITRE 2 : DISPOSITIONS PARTICULIERES

Article 1 : Objet de l'appel d'offres

Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Article 06 § C : Liste des pièces exigées pour le dossier technique

C1. Une note indiquant **les moyens humains et techniques** du concurrent et mentionnant éventuellement,

- La date,
- Le lieu,
- La nature et l'importance des prestations à l'exécution desquelles le concurrent a participé et la qualité de sa participation.

C2. Les attestations de référence originales ou leurs copies certifiées conformes à l'original délivrées par les maîtres d'ouvrage publics ou privés ou par les hommes de l'art sous la direction desquels le concurrent a exécuté des prestations d'importance et de complexité similaires à celles des prestations objet du présent appel d'offres, **dont au moins une (01) attestation de référence relative à des prestations d'intégration des solutions cyber sécurité de 9 000 000,00 DHS TTC.**

- La nature des prestations ;
- Leur montant ;
- Le nom et la qualité du signataire et son appréciation.
- L'année de réalisation (**entre 2014 et 2024**).

Article 06 § D : Liste des pièces exigées pour le dossier additif

- Aucun dossier additif n'est exigé

Article 08 : Liste des pièces exigées pour l'offre technique

1. La méthodologie de gestion que le concurrent compte déployer pour la bonne gestion des prestations ;
2. Les attestions des éditeurs Pour les solutions proposées autorisant le soumissionnaire à répondre à cet Appel d'Offres
3. Un Engagement de renouvellement du support auprès de l'éditeur durant la période de Maintenance.
4. Un état récapitulatif de la solution proposée avec spécifications techniques ;
5. Les CV nominatifs de tous les intervenants en précisant les diplômes, les qualités et les anciennetés dans le domaine objet de l'appel d'offres.

Les membres du projet doivent comprendre au moins :

Un (01) Chef de projet : Bac+5 en management des SI, Ingénierie des SI ou équivalent ayant les compétences suivantes :

- ✓ Ayant au **moins huit (8) ans** d'expérience dans la gestion de projets de sécurité complexes et de grandes envergures.
- ✓ Disposant obligatoirement des certifications suivantes : PMP et CISSP

Un (01) expert intégration WAF: Bac +5 en informatique ou sécurité SI ou équivalent, ayant au moins **dix (10) ans** d'expérience dans le domaine de sécurité informatique et disposant obligatoirement des certifications suivantes : CISSP et ISO27001 LA

La certification professionnelle de la solution proposée représente un plus.

Un (01) expert intégration solution durcissement : Bac +5 en informatique ou Sécurité SI ou équivalent, ayant au moins **5 ans** d'expérience dans le domaine de sécurité informatique et disposant obligatoirement des certifications suivantes : CEH (Certified Ethical Hacking) ou équivalent (CPTE de mile2, CSSP…) ;

La certification professionnelle de la solution proposée représente un plus.

Un (01) expert intégration concentrateur VPN : Bac +5 en informatique ou Sécurité SI ou équivalent, ayant au moins **5 ans** dans le domaine de sécurité informatique

La certification professionnelle de la solution proposée représente un plus.

Trois (03) expert intégration NAC : Bac +5 en informatique ou Sécurité SI ou équivalent, ayant au moins **5 ans** d'expériences dans le domaine de sécurité informatique.

La certification professionnelle de la solution proposée représente un plus.

Article 16 : Critères d'admissibilité des concurrents et d'attribution du marché

Le seul critère d'attribution, après admission, est l'**offre la moins-disante** sur la base **du prix global combinant le prix de la tranche ferme et le prix de la tranche conditionnelle pour les trois années.**

ANNEXE I : MODELE DE DECLARATION SUR L'HONNEUR

Déclaration sur l'honneur

- Référence de l'appel d'offres : **088-24-AOO**
- Mode de passation : **Appel d'offres Ouvert**
- Objet du marché : **Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information**
  - **Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information**
  - **Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information**

A – Si le concurrent est une personne physique

Je, soussigné : .....(prénom, nom et qualité)
Numéro de tél……numéro du fax……adresse électronique……..

Agissant en mon nom personnel et pour mon propre compte,
-Adresse du domicile élu : .....
-Affilié à la CNSS sous le n° : ..... (1)
-Inscrit au registre du commerce de.....(localité) sous le n° ..... (1)
-N° de patente..... (1)
-N° du compte courant postal/bancaire ou à la TGR……(RIB)

B - Si le concurrent est une personne morale

Je, soussigné .....(prénom, nom et qualité au sein de l'entreprise)
numéro de tél……numéro du fax……adresse électronique……..…

-Agissant au nom et pour le compte de..... (raison sociale **(**)** et forme juridique de la société) au capital de : .....
-Adresse du siège social de la société : .....
-Adresse du domicile élu.....
-Affiliée à la CNSS sous le n°.....(1)
-Inscrite au registre du commerce.....localité) sous le n°.....(1)
-N° de patente.....(1)
-N° du compte courant postal-bancaire ou à la TGR……(RIB)

En vertu des pouvoirs qui me sont conférés déclare sur l'honneur :

1) M'engager à couvrir, dans les limites fixées dans le cahier des charges, par une police d'assurance, les risques découlant de mon activité professionnelle ;

2) Que je remplie les conditions prévues à l'article 24 du règlement des marchés publics de l'ONDA ;

3) Étant en redressement judiciaire j'atteste que je suis autorisé par l'autorité judiciaire compétente à poursuivre l'exercice de mon activité (2) ;

4) M'engager, si j'envisage de recourir à la sous-traitance :

a) A m'assurer que les sous-traitants remplissent également les conditions prévues par l'article 24 du règlement des marchés publics de l'ONDA ;

b) Que celle-ci ne peut dépasser 50 % du montant du marché, ni porter sur les prestations constituant le lot ou le corps d'état principal prévues dans le cahier des prescriptions spéciales, ni sur celles que le maître d'ouvrage a prévu dans ledit cahier ;

5) M'engager à ne pas recourir par moi-même ou par personne interposée à des pratiques de fraude ou de corruption de personnes qui interviennent à quelque titre que ce soit dans les différentes procédures de passation, de gestion et d'exécution du présent marché.

6) M'engager à ne pas faire, par moi-même ou par personnes interposées, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion du présent marché.

7) Attester que je ne suis pas en situation de conflit d'intérêt tel que prévu à l'article 151 du règlement des marchés publics de l'ONDA.

8) Certifier l'exactitude des renseignements contenus dans la présente déclaration sur l'honneur et dans les pièces fournies dans mon dossier de candidature.

9) Reconnaitre avoir pris connaissance des sanctions prévues par l'article 142 du règlement des marchés publics de l'ONDA, relatives à l'inexactitude de la déclaration sur l'honneur.

Fait à.....le.....

Signature et cachet du concurrent

(1) pour les concurrents non installés au Maroc, préciser la référence aux documents équivalents lorsque ces documents ne sont pas délivrés par leur pays d'origine ou de provenance.

(2) à supprimer le cas échéant.

NB : Pour les groupements, chaque membre du groupement doit présenter sa propre déclaration sur l'honneur.

(**) La raison sociale doit être identique à celle figurant sur les statuts de la société

ANNEXE II : MODELE D'ACTE D'ENGAGEMENT

Acte d'engagement

Appel d'offres ouvert sur offres des prix n° **088-24-AOO** du **jeudi 11 juillet 2024**.

A - Partie réservée à l'ONDA

Objet du marché : **Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information**
Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Passé en application des dispositions de l'alinéa 2, paragraphe 1 de l'article 16 et de l'alinéa 3, paragraphe 3 de l'article 17 du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

B - Partie réservée au concurrent

a) Si le concurrent est une personne physique

Je, soussigné : .....(prénom, nom et qualité)
Numéro de tél……numéro du fax……adresse électronique……..

Agissant en mon nom personnel et pour mon propre compte,
- Adresse du domicile élu : .....
- Affilié à la CNSS sous le n° : ..... (2)
- Inscrit au registre du commerce de.....(localité) sous le n° ..... (2)
- N° de patente..... (2)

b) Si le concurrent est une personne morale

Je, soussigné .....(prénom, nom et qualité au sein de l'entreprise)
Numéro de tél…….numéro du fax……adresse électronique……..…

- Agissant au nom et pour le compte de..... (raison sociale **(**)** et forme juridique de la société) au capital de : .....
- Adresse du siège social de la société : .....
- Adresse du domicile élu.....
- Affiliée à la CNSS sous le n°.....(2)
- Inscrite au registre du commerce.....localité) sous le n°.....(2)
- N° de patente.....(2)(3)

En vertu des pouvoirs qui me sont conférés :

Après avoir pris connaissance du dossier de consultation concernant les prestations précisées en objet de la partie A ci-dessus ;

Après avoir apprécié à mon point de vue et sous ma responsabilité la nature et les difficultés que comportent ces prestations :

- Remets, revêtu (s) de ma signature un bordereau de prix, un détail estimatif et/ou la décomposition du montant global) établi (s) conformément aux modèles figurant au dossier de consultation ;

- M'engage à exécuter lesdites prestations conformément au cahier des prescriptions spéciales et moyennant les prix que j'ai établis moi-même, lesquels font ressortir :

Tranche ferme :

- Montant hors T.V.A. Y COMPRIS DROITS DE DOUANES : ..... (en chiffres et en lettres) ;
- Taux de la T.V.A. : **20**% ;
- Montant de la T.V.A. : ..... (en chiffres et en lettres) ;
- Montant T.V.A. comprise : ..... (en chiffres et en lettres).

Tranche conditionnelle :

- Montant annuel hors T.V.A. : ..... (en chiffres et en lettres) ;
- Taux de la T.V.A. : **20**% ;
- Montant de la T.V.A. : ..... (en chiffres et en lettres) ;
- Montant annuel T.V.A. comprise : ..... (en chiffres et en lettres).

L'Office National des Aéroports se libérera des sommes dues par lui en faisant donner crédit au compte ..... (à la trésorerie générale, bancaire, ou postal) ouvert à mon nom (ou au nom de la société) à ..... (Localité), sous relevé d'identification bancaire (RIB) numéro .....

Fait à.....le.....
(Signature et cachet du concurrent)

1) Lorsqu'il s'agit d'un groupement, ses membres doivent :
   a) Mettre : «Nous, soussignés..... nous obligeons conjointement/ou solidairement (choisir la mention adéquate et ajouter au reste de l'acte d'engagement les rectifications grammaticales correspondantes) ;
   b) Ajouter l'alinéa suivant : « désignons..... (prénoms, noms et qualité) en tant que mandataire du groupement ».
   c) **Préciser la ou les parties** des prestations que chacun des membres du groupement s'engage à réaliser **pour le groupement conjoint** et éventuellement pour le groupement solidaire (optionnel).
2) Pour les concurrents non installés au Maroc, préciser la référence des documents équivalents et lorsque ces documents ne sont pas délivrés par leur pays d'origine, la référence à la déclaration délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.
3) Ces mentions ne concernent que les personnes assujetties à cette obligation.

(**) La raison sociale doit être identique à celle figurant sur les statuts de la société

ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) –TF

AO N° : 088-24-AOO

Objet : Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

N°ITEMS	DESIGNATIONS DES OUVRAGES	UDM	QTE	PU HORS TVA EN CHIFFRES (*)	PT HORS TVA EN CHIFFRES (*)
1	Fourniture et mise en place d'une solution WAF	FORFAIT	1		
2	Fourniture et mise en place d'une solution de durcissement des configurations	U	1000		
3	Mise en place d'un concentrateur VPN	U	1000		
4	Mise en place d'une solution NAC	U	3000		
TOTAL HORS TVA Y COMPRIS DROITS DE DOUANES (A)					
DONT MONTANT DROITS DE DOUANE					
TVA 20% (B)					
TOTAL TVA COMPRISE (A+B)					

(*) Le concurrent doit préciser le libellé de la monnaie conformément au règlement de la consultation.

ANNEXE III : MODELE BORDEREAU DES PRIX – DETAIL ESTIMATIF (BDP-DE) – TC

AO N° : 088-24-AOO

Objet : Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

N°ITEMS	DESIGNATIONS DES OUVRAGES	UDM	QTE	PU HORS TVA EN CHIFFRES (*)	PT HORS TVA ANNUEL EN CHIFFRES (*)
1	Maintenance de la solution WAF	Forfait Trimestriel	4		
2	Maintenance de la solution de durcissement des configurations	Forfait Trimestriel	4		
3	Maintenance du concentrateur VPN	Forfait Trimestriel	4		
4	Maintenance de la solution NAC	Forfait Trimestriel	4		
TOTAL ANNUEL HORS TVA (A)					
TVA 20% (B)					
TOTAL ANNUEL TVA COMPRISE (A+B)					

(*) Le concurrent doit préciser le libellé de la monnaie conformément au règlement de la consultation.

ROYAUME DU MAROC
OFFICE NATIONAL DES AEROPORTS

المكتب الوطني للمطارات
Office National Des Aéroports

CAHIER DES PRESCRIPTIONS SPECIALES

Appel d'offres ouvert N° 088-24-AOO

Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

CAHIER DES PRESCRIPTIONS SPECIALES 5

CHAPITRE 1 : CLAUSES ADMINISTRATIVES 5

ARTICLE 01 : OBJET DU MARCHE 5
ARTICLE 02 : MODE DE PASSATION DU MARCHE 5
ARTICLE 03 : TYPE DU MARCHE 5
ARTICLE 04 : DECOMPOSITION EN TRANCHES 5
ARTICLE 05 : INDEMNITES 5
ARTICLE 06 : PIECES CONSTITUTIVES DU MARCHE 5
ARTICLE 07 : CONNAISSANCE DU DOSSIER 6
ARTICLE 08 : REFERENCES AUX TEXTES GENERAUX 6
ARTICLE 09 : RESILIATION 6
ARTICLE 10 : DOMICILE DU PRESTATAIRE 7
ARTICLE 11 : REGLEMENT DES DIFFERENDS 7
ARTICLE 12 : CAS DE FORCE MAJEURE 7
ARTICLE 13 : ENTREE EN VIGUEUR ET APPROBATION 7
ARTICLE 14 : NANTISSEMENT 7
ARTICLE 15 : FORMALITE D'ENREGISTREMENT 8
ARTICLE 16 : DROIT APPLICABLE 8
ARTICLE 17 : DROITS ET TAXES 8

CHAPITRE 2 : CLAUSES TECHNIQUES –Tranche ferme – 10

ARTICLE 01 : MAITRE D'ŒUVRE 10
ARTICLE 02 : GARANTIE PARTICULIAIRE 10
ARTICLE 03 : NATURE DES PRESTATIONS ET REVISION DES PRIX 10
ARTICLE 04 : DELAI D'EXECUTION 10
ARTICLE 05 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE 10
ARTICLE 06 : DELAI DE GARANTIE 11
ARTICLE 07 : RECEPTION DES PRESTATIONS 11
ARTICLE 08 : MODE DE PAIEMENT 11
ARTICLE 09 : PENALITES POUR RETARD 12
ARTICLE 10 : BREVETS 12
ARTICLE 11 : LOIS ET NORMES 12
ARTICLE 12 : CONSISTANCE DES PRESTATIONS 13
ARTICLE 13 : CONTROLE ET VERIFICATION 38
ARTICLE 14 : DEFINITION DES PRIX 38

CHAPITRE 3 : CLAUSES TECHNIQUES – Tranche conditionnelle- 39

ARTICLE 01 : MAITRE D'ŒUVRE 39
ARTICLE 02 : NATURE DES PRESTATIONS ET REVISION DES PRIX 39
ARTICLE 03 : DUREE DU MARCHE 39
ARTICLE 04 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE - TRANCHE CONDITIONNELLE 39
ARTICLE 05 : DELAI DE GARANTIE 39
ARTICLE 06 : RECEPTION DES PRESTATIONS DE TRANCHE CONDITIONNELLE 39
ARTICLE 07 : MODE DE PAIEMENT 40
ARTICLE 08 : PENALITES POUR RETARD 40
ARTICLE 09 : BREVETS 40
ARTICLE 10 : NORMES 40
ARTICLE 11 : GARANTIE PARTICULIERE 40

ARTICLE 12 : DESCRIPTION TECHNIQUE DES PRESTATIONS 41
ARTICLE 13 : CONTROLE ET VERIFICATION 42
ARTICLE 14 : DEFINITION DES PRIX 43

ENTRE :

L'OFFICE NATIONAL DES AEROPORTS, désigné ci-après, par le sigle « O.N.D.A. », représenté par sa Directrice Générale, faisant élection de domicile à l'Aéroport Casablanca Mohammed V - Nouaceur.

d'une part,

ET :
(Titulaire)
Faisant élection de domicile à
Inscrite au Registre de Commerce de sous le n°
Affiliée à la CNSS sous le n°
Représentée par _____ en vertu des pouvoirs qui lui sont conférés,

D'autre part,

CAHIER DES PRESCRIPTIONS SPECIALES
CHAPITRE 1 : CLAUSES ADMINISTRATIVES

ARTICLE 01 : OBJET DU MARCHE

Le présent marché a pour objet : **Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information,**

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tel que décrit dans les clauses techniques du présent Cahier des Prescriptions Spéciales.

ARTICLE 02 : MODE DE PASSATION DU MARCHE

Le présent marché est passé en application des dispositions de **l'alinéa 2, paragraphe 1 de l'article 16 et de l'alinéa 3, paragraphe 3 de l'article 17** du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

ARTICLE 03 : TYPE DU MARCHE

Le présent marché est un marché à tranches conditionnelles pour lequel il est prévu une tranche ferme couverte par un crédit budgétaire disponible et que le prestataire est certain de réaliser, et une tranche conditionnelle dont l'exécution est subordonnée par la disponibilité du crédit budgétaire et à la notification de l'ordre de service prescrivant le commencement des prestations y afférentes, dans les délais prévus par le présent marché.

ARTICLE 04 : DECOMPOSITION EN TRANCHES

Le présent marché comporte les tranches suivantes :

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

ARTICLE 05 : INDEMNITES

5.1 Indemnité de dédit : en cas de renonciation par le maître d'ouvrage à réaliser la tranche conditionnelle, il ne sera pas versé d'indemnité de dédit au prestataire.
5.2 Indemnité d'attente : Lorsque l'ordre de service afférent à la tranche conditionnelle n'a pu être donné dans les délais prescrit dans le présent marché, aucune indemnité d'attente ne sera versée au titulaire. Néanmoins, le titulaire a le droit de demander la résiliation de la tranche conditionnelle au cas où la notification de l'ordre de service de commencement dépassera trois (3) mois suivant la date prévue de commencement.

ARTICLE 06 : PIECES CONSTITUTIVES DU MARCHE

Les pièces constitutives du présent marché sont :

1) L'acte d'engagement ;
2) Le présent cahier des prescriptions spéciales (CPS) ;
3) Le Bordereau Des Prix – Détail Estimatif : (BDP-DE) ;

4) Les pièces constitutives de l'offre technique ;
5) Le CCAG-T pour **la tranche ferme** ;
6) Le CCAG-EMO pour la **tranche conditionnelle**.

ARTICLE 07 : CONNAISSANCE DU DOSSIER

Les spécifications et les prescriptions techniques relatives aux prestations à réaliser sont contenues dans le présent marché, l'entrepreneur déclare :

- Avoir pris pleine connaissance de l'ensemble des prestations ;
- Avoir fait préciser tous points susceptibles de contestations ;
- Avoir fait tous calculs et sous détails ;
- N'avoir rien laissé au hasard pour déterminer le prix de chaque nature de prestations présentées par elle et pouvant donner lieu à discussion.
- Avoir apprécié toutes les difficultés qui pourraient se présenter lors de l'exécution des prestations objet du présent marché et pour lesquelles aucune réclamation ne sera prise en considération.

ARTICLE 08 : REFERENCES AUX TEXTES GENERAUX

Le présent marché est soumis aux prescriptions relatives aux marchés publics notamment celles définies par :

- Le règlement relatif aux marchés publics de l'Office National des Aéroports approuvé le 09 Juillet 2014 et la décision de son amendement réf 01/RM/2015 du 02 avril 2015 ;
- Le décret N° 2-14-394 du 6 Chaabane 1437 (13 Mai 2016) approuvant le cahier des clauses administratives générales, applicables aux marchés de travaux exécutés pour le compte de l'Etat, pour les prestations à réaliser dans le cadre de **la tranche ferme** du présent marché ;
- Le décret N° 2-01-2332 du 22 Rabii I 1423 (04 juin 2002) approuvant le cahier des clauses administratives générales, applicables aux marchés d'études et de maîtrises d'œuvres (CCAG EMO) exécutés pour le compte de l'Etat, pour les prestations à réaliser dans le cadre de **la tranche conditionnelle** du présent marché ;
- Tous les textes législatifs et règlementaires concernant l'emploi et les salaires de la main d'œuvre ;
- Les lois et règlements en vigueur au Maroc à la date de la signature du présent marché.

Bien que non jointes au présent CPS, le titulaire est réputé connaître tous textes ou documents techniques applicables au présent marché. Le titulaire ne peut se prévaloir dans l'exercice de sa mission d'une quelconque ignorance de ces textes et, d'une manière générale, de toute la réglementation intéressant les prestations en question.

ARTICLE 09 : RESILIATION

Dans le cas où le titulaire aurait une activité insuffisante ou en cas de la non-exécution des clauses du présent marché, l'Office National Des Aéroports le mettrait en demeure de satisfaire à ses obligations, si la cause qui a provoqué la mise en demeure subsiste, le marché pourra être résilié sans aucune indemnité sous peine d'appliquer les mesures coercitives prévues par les articles 79 et 80 du CCAG-T et/ou par l'article 52 du CCAG-EMO selon la tranche concernée du présent marché.

L'ONDA se réserve le droit de résilier le marché dans le cas de modifications importantes ne pouvant être prises en charge dans le cadre du présent marché conformément à la réglementation en vigueur.

ARTICLE 10 : DOMICILE DU PRESTATAIRE

L'entrepreneur est tenu d'élire domicile au Maroc qu'il doit indiquer dans l'acte d'engagement ou le faire connaître au maître d'ouvrage dans le délai de quinze (15) jours à partir de la notification, qui lui est faite, de l'approbation de son marché en application des dispositions de l'article 136 du règlement relatif aux marchés publics de l'Office National des Aéroports en vigueur.

Faute par lui d'avoir satisfait à cette obligation, toutes les notifications qui se rapportent au marché sont valables lorsqu'elles ont été faites au siège de l'entreprise dont l'adresse est indiquée dans le présent marché.

En cas de changement de domicile, l'entrepreneur est tenu d'en aviser le maître d'ouvrage, par lettre recommandée avec accusé de réception, dans les quinze (15) jours suivant la date d'intervention de ce changement.

ARTICLE 11 : REGLEMENT DES DIFFERENDS

Tout litige entre l'Office National Des Aéroports et le prestataire sera soumis aux tribunaux compétents de Casablanca « MAROC ».

ARTICLE 12 : CAS DE FORCE MAJEURE

En cas de survenance d'un événement de force majeure, les dispositions applicables sont celles définies par l'article 47 du C.C.A.G.T pour les prestations à réaliser dans le cadre de **la tranche ferme** du présent marché et l'article 32 du CCAG-EMO pour les prestations à réaliser dans le cadre de **la tranche conditionnelle** dudit marché.

ARTICLE 13 : ENTREE EN VIGUEUR ET APPROBATION

L'entrée en vigueur du présent marché interviendra après son approbation par l'autorité compétente et la notification au titulaire.

ARTICLE 14 : NANTISSEMENT

En cas de nantissement, les dispositions applicables sont celles prévues par la loi n° 112-13 relative au nantissement des marchés publics promulguée par le Dahir n°1-15-05 du 29 rabii II 1436 (19 février 2015).

En vue de l'établissement de l'acte de nantissement, le maître d'ouvrage remet au titulaire du marché, sur demande et sans frais, une copie du marché portant la mention « EXEMPLAIRE UNIQUE » dûment signée et indiquant que ladite copie est délivrée en unique exemplaire destiné à former titre pour le nantissement du marché, et ce conformément aux dispositions de l'article 4 de la loi n°112-13 susmentionnée.

Le responsable habilité à fournir au titulaire du marché ainsi qu'au bénéficiaire du nantissement ou de subrogation les renseignements et les états prévus à l'article 8 de la loi n° 112-13 est le Directeur ou la Directrice Général(e) de l'ONDA.

Le Directeur ou la Directrice Général(e) de l'ONDA et/ou toute autre personne désignée par lui/elle sont seul(e)s habilité(e)s à effectuer les paiements au nom de l'ONDA entre les mains du bénéficiaire du nantissement ou de la subrogation, conformément à la législation et à la réglementation en vigueur.

ARTICLE 15 : FORMALITE D'ENREGISTREMENT

Le titulaire s'engage à présenter le présent marché à la formalité d'enregistrement dans un délai de **30 jours** à compter de la date de la notification de son approbation conformément à la réglementation en vigueur. L'original du marché enregistré sera conservé par l'Office National Des Aéroports.

ARTICLE 16 : DROIT APPLICABLE

Le marché sera interprété conformément au droit Marocain.

ARTICLE 17 : DROITS ET TAXES

Les prix du présent marché s'entendent Toutes Taxes Comprises Delivered Duty Paid (TTC DDP).

Le prestataire (Entrepreneur, fournisseur ou prestataire de service) est réputé avoir parfaitement pris connaissance de la législation fiscale en vigueur au Maroc. Par conséquent, il supportera, par défaut, tous les impôts et taxes dont il est redevable au Maroc, y compris la TVA, tous droits de douane, de port ou autres.

Les **prestations de service** réalisées pour le compte de l'ONDA par une entreprise non résidente sont soumises à l'impôt sur les sociétés au taux de **10%** de ces prestations. Cet impôt est prélevé du montant desdites prestations sous forme de retenue à la source. **Une copie de l'attestation du versement** de cet impôt sera remise au prestataire, à sa demande.

Pour les entreprises originaires de pays ayant signé avec le Maroc une convention destinée à éviter les doubles impositions, la retenue à la source est déductible des impôts dus dans leur pays d'origine.

Pour les prestations à réaliser dans le cadre de la tranche ferme du marché, l'ONDA prendra en charge le paiement des impôts et taxes à l'importation y compris les droits et accessoires de douane et la TVA à l'importation **figurant sur la fiche de liquidation émise par les services de la douane**, **hors** les frais de la logistique (Transitaire, emmagasinage et surestaries le cas échéant) qui restent à la charge du prestataire y compris la gestion de la logistique d'importation.

Dans le cas où le Cahier des Prescriptions Spéciales prévoit le paiement par lettre de crédit et le prestataire opterait pour ce mode de paiement, le montant des droits et taxes en question sera déduit du montant du CREDOC.

Si l'ONDA paierait des frais supplémentaires, pour quelle que raison que ce soit, à cause d'un motif imputable au fournisseur, l'ONDA déduira d'office lesdits frais des sommes dues au fournisseur.

Aussi, en cas de déclaration douanière faisant ressortir des montants supérieurs à ceux indiqués au présent Marché, le supplément de droits et taxes de douane résultant de cette différence de déclaration sera à la charge du Fournisseur.

En cas d'augmentation des sommes à valoir pour la couverture des droits de douane et taxes à l'importation, l'ONDA prendra les engagements complémentaires nécessaires pour couvrir lesdites sommes, conformément à la réglementation en vigueur.

CHAPITRE 2 : CLAUSES TECHNIQUES –Tranche ferme –

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

N.B : Les éventuels marques commerciales, références au catalogue, appellations, brevets, conception, types, origines ou producteurs particuliers mentionnés dans les clauses techniques sont données à titre indicatif. Le cas échéant, le prestataire peut les substituer par toute autre proposition ayant des caractéristiques équivalentes et qui présentent une performance et qualité égales ou supérieures à celles qui sont exigées.

ARTICLE 01 : MAITRE D'ŒUVRE

Le maitre d'œuvre de la présente tranche du marché est la **Direction des Systèmes d'Information**.

ARTICLE 02 : GARANTIE PARTICULIAIRE

Le Prestataire garantit que toutes les fournitures livrées en exécution du marché sont neuves, n'ont jamais été utilisées, sont du modèle le plus récent en service et incluent toutes les dernières améliorations en matière de conception et de matériaux, sauf si le marché en a disposé autrement. Le fournisseur garantit en outre que les fournitures livrées en exécution du marché n'auront aucune défectuosité due à leur conception, aux matériaux utilisés ou à leur mise en œuvre (sauf dans la mesure où la conception ou le matériau est requis par les spécifications du Maître d'Ouvrage) ou à tout acte ou omission du fournisseur, survenant pendant l'utilisation normale des fournitures livrées dans les conditions prévalant dans le pays de destination finale.
Le Maître d'ouvrage notifiera au prestataire par écrit toute réclamation faisant jouer cette garantie.
A la réception d'une telle notification, le prestataire, dans un délai de trois (03) semaines, remplacera les fournitures non conformes sans frais pour le maître d'ouvrage.
Si le prestataire, après notification, manque à se conformer à la notification du maître d'ouvrage, dans un délai de deux (02) semaines, ce dernier applique les mesures coercitives nécessaires, aux risques et frais du fournisseur et sans préjudice de tout autre recours de l'acquéreur contre le fournisseur en application des clauses du marché.

ARTICLE 03 : NATURE DES PRESTATIONS ET REVISION DES PRIX

La présente tranche du marché concerne **la fourniture** dont les prix applicables sont fermes et non révisables.

ARTICLE 04 : DELAI D'EXECUTION

Le d'exécution de la présente tranche du marché est fixé à **huit (8) mois** à compter de la date de l'ordre de service prescrivant le commencement des prestations établi et notifié au titulaire.

ARTICLE 05 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE

a) Cautionnement : Le cautionnement définitif est fixé à **Trois pour cent (3%)** du montant initial de la présente tranche du marché arrondi au dirham supérieur conformément aux dispositions de l'article 15 du C.C.A.G.T.

b) Retenue de garantie : Les Dispositions relatives à la retenue de garantie telles que définies aux articles 16 et 64 du C.C.A.G.T sont seules applicables.

Toutes les cautions présentées sous forme de cautions personnelles et solidaires doivent contenir la mention « à première demande de l'ONDA » et être émises par un organisme Marocain agréé.

ARTICLE 06 : DELAI DE GARANTIE

Le délai de garantie est fixé à **douze (12) mois** à compter de la date de la réception provisoire. Durant la période de garantie, le prestataire est soumis aux dispositions arrêtées par l'article 75 du CCAGT.

Cette garantie couvre aussi bien l'entretien, l'assistance, l'intervention sur site, les pièces de rechange et la main d'oeuvre sur les logiciels et les équipements installés par le prestataire.
La garantie couvre tous les frais nécessaires à la réparation et au remplacement des pièces de rechange ou matériel défectueux. Elle couvre aussi les frais de main d'oeuvre, de déplacement du personnel d'entretien et tous les frais annexes.
En cas de dysfonctionnement du système, l'ONDA avisera le prestataire par écrit (fax ou email) ou par téléphone sur les anomalies constatées. A cet effet, le prestataire devra intervenir sur site dans un délai maximal de 04 heures après la notification et devra déployer tous les moyens humains et matériels nécessaires pour pallier au problème notifié dans les délais impartis.
Le prestataire garantira qu'au moins un interlocuteur, formé sur les installations, est joignable et disponible **24/24h, 7/7j et 365 jours/an**. Le prestataire se chargera de l'affectation et de changement des ressources nécessaires pour assurer le contact en continu avec l'ONDA. Un tableau de service doit être dressé au début de la garantie à cet effet. Tout éventuel changement doit être communiqué à l'ONDA pour garantir la disponibilité exigée.

ARTICLE 07 : RECEPTION DES PRESTATIONS

Réception Provisoire :

Un Procès-verbal de réception provisoire sera établi par les personnes habilitées de l'ONDA dès que toutes les vérifications et tests auront été déclarés satisfaisants conformément aux dispositions définies par l'article 73 du CCAGT.

Réception Définitive :

Conformément aux dispositions de l'article 76 du C.C.A.G.T, la réception définitive sera prononcée **douze (12) mois** après la date du procès-verbal de la réception provisoire.

ARTICLE 08 : MODE DE PAIEMENT

L'ONDA se libérera des sommes dues en exécution de la présente tranche du marché en faisant donner crédit au compte ouvert au nom du prestataire indiqué sur l'acte d'engagement.

Les paiements seront effectués par virement bancaire ou par une lettre de crédit irrévocable et confirmée par la banque du fournisseur.

Si le prestataire opte pour le paiement par lettre de crédit, tous les frais et accessoires relatifs à l'ouverture de la lettre de crédit sont à la charge du fournisseur.

Lorsque le règlement n'est pas prévu par lettre de crédit, le paiement des sommes dues est effectué dans un délai maximum de **quatre-vingt-dix jours (90)** à compter de la date de réception des prestations demandées sur présentation de factures en cinq (5) exemplaires.

Dispositions relatives à la facturation :

- Les factures doivent être émises au plus tard le dernier jour du mois de la réalisation des prestations objet du présent marché.
- Les factures doivent se conformer aux dispositions règlementaires notamment les articles 145 alinéa III et 146 du Code Général des Impôts Marocain en vigueur.
- Les factures doivent porter les dates de leur établissement.
- En cas de remise tardive de la facture générant ainsi une sanction pécuniaire, au profit du Trésor, à l'encontre de l'ONDA, le montant de ladite sanction pécuniaire sera déduit, le cas échéant, à l'identique des sommes dues au prestataire.

ARTICLE 09 : PENALITES POUR RETARD

A défaut par l'Entrepreneur d'avoir exécuté à temps la présente tranche du marché ou d'avoir respecté tout planning ou délai prévu par la présente tranche du marché, il lui sera appliqué sans préjudice de l'application des mesures prévues par les articles 79 et 80 du CCAGT, une pénalité de **cinq pour mille** (**5 ‰**) du montant initial de la présente tranche du marché éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux, par jour de retard.

1- **En cas de retard dans l'exécution des travaux :** Par application de l'article 65 du CCAGT la pénalité est plafonnée à **huit pour Cent (8 %)** du montant initial du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux ; au-delà de ce plafond, l'O.N.D.A. se réserve le droit de procéder à la résiliation du marché sans préjudice des mesures coercitives prévues par les articles 79 et 80 C.C.A.G.T.

2- **En cas de retard dans la remise des documents ou rapports ou pour défaut de réalisation de certaines de ses obligations :** Par application de l'article 66 du CCAGT la pénalité est plafonnée à **deux pour Cent (2 %)** du montant initial du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse des travaux.

Les sommes concernant les pénalités seront déduites des décomptes de l'entreprise sans qu'il ne soit nécessaire d'une mise en demeure préalable.

ARTICLE 10 : BREVETS

Le prestataire garantira le maître d'ouvrage contre toute réclamation des tiers relative à la contrefaçon ou à l'exploitation non autorisée d'une marque commerciale ou de droit d'auteur résultant de l'emploi des prestations ou d'un de leurs éléments.

ARTICLE 11 : LOIS ET NORMES

Les prestations livrées en exécution du marché doivent être conformes aux lois et normes Marocaines suivantes :

- Loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
- Loi n°53-05 relative à l'échange électronique de données juridiques ;
- Loi n°07- 03 complétant le code pénal en ce qui concerne la répression des infractions relatives aux systèmes informatiques ;
- Loi n°02-00 relative aux droits d'auteur au Maroc ;
- Loi n°05-20 relative à la Cybersécurité et son décret d'application (n° 2-21-406) ;

- Loi n°43-20 relative à l'utilisation des signatures électroniques ;
- Loi n°66-99 relative aux archives ;
- La Directive Nationale de la Sécurité des Systèmes d'Information.

ARTICLE 12 : CONSISTANCE DES PRESTATIONS

a. AQ1 : Acquisition et mise d'une solution WAF (Web Application Firewall)

La solution recherchée :

- La solution recherchée doit permettre un déploiement On-Premise
- La solution proposée doit être capable d'évoluer en utilisant des clusters de plus de deux nœuds.
- La solution proposée doit supporter les 3 modes d'opérations ci-dessous :
  - Bypass : Mode dont les appliances sont Running, mais pas de detection ni d'interception d'intrusion
  - Passive : Full detection d'intrusion
  - Active : Full detection et interception d'intrusion
- La solution souhaitée doit etre capable d'agit comme un Out-Of-Path Monitor ou un Bridge Transparent
- La solution recherchée doit être sous format d'Appliance physique en HA
- La solution souhaitée doit etre une partie intégrante d'une solution ADC
- La solution proposée doit prendre en charge des politiques de sécurité prêtes à l'emploi basées sur un modèle de sécurité négatif traitant d'un large éventail de menaces de sécurité.
- La solution souhaitée doit prendre en charge la spécification d'un répertoire virtuel sur le serveur Web et d'un groupe de filtres de sécurité à appliquer à une application Web (Virtual path)
- La solution proposée doit etre capable d'agir comme un proxy inverse
- La solution doit être capable d'assurer la protection contre les dix principales vulnérabilités OWASP en matière de sécurité des applications Web :
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - XML External Entities
  - Broken Access Control
  - Security Misconfiguration
  - Cross-Site Scripting (XSS)
  - Insecure Deserialization
  - Using Components with Known Vulnerabilities
  - Insufficient Logging & Monitoring
- La solution doit être capable d'assurer la protection contre la classification des attaques de Sécurité Web WASC
- La solution doit être capable d'assurer la protection contre les menaces ci-dessous :
  - SQL injection Cross-site scripting (XSS)
  - Cross-Site-Request-Forgery (CSRF)
  - Parameter tampering
  - Hidden-field manipulation
  - Session manipulation
  - Cookie poisoning Stealth commanding
  - Backdoor and debug options
  - Application-buffer-overflow attacks
  - Brute-force attacks
  - Data encoding Unauthorized navigation

  - SOAP- and Web-services manipulation
  - Web Scraping
  - API Protections
  - OS command injections
  - LDAP injections
  - SSI injections
  - XPath injections
  - Sensitive information leakage (e.g., CCN, SSN, custom defined)
  - Application DoS
  - From field manipulation
  - Session hijacking
  - Access to predictable resource locations
  - Unauthorized navigation
  - Web server reconnaissance
  - Directory/path traversal
  - Forceful browsing
  - Hotlink
  - HTTP response splitting
  - Evasion and illegal encoding
  - XML validation
  - Web services method restrictions and validation
  - HTTP RFC violations
  - HTTP request format and limitation violations (size, unknown method, etc.)
  - Use of revoked or expired client certificates
  - File upload violations
- La solution souhaitée doit prendre en charge l'application de politiques quel que soit le codage des caractères afin de lutter contre les techniques d'évasion, telles que :
  - URL-decoding (for example, %XX)
  - Self-referencing paths (that is,. use of /./ and encoded equivalents)
  - Path back-references (that is, use of /../ and encoded equivalents)
  - Mixed case
  - Excessive use of whitespace
  - Comment removal (for example, convert DELETE/**/FROM to DELETE FROM)
  - Conversion of (Windows-supported) backslash characters into forward slash characters.
  - Conversion of IIS-specific Unicode encoding (%uXXYY) IIS extended
  - Unicode
  - Virtual directory route positive folder enforcement
  - Base64 Encoding
- La solution souhaitée doit prendre en charge l'application des flux de requêtes via l'application, garantissant que le flux d'un utilisateur via l'application, d'une page à la suivante, est cohérent avec le comportement attendu
- La solution proposée doit être capable de fonctionner en utilisant un modèle de sécurité positif en apprenant ou en définissant des règles décrivant le comportement attendu d'une application ou d'un service et en bloquant tout le trafic qui ne correspond pas à ces règles.
- La solution proposée ne doit pas nécessiter de mises à jour des signatures pour se protéger contre les nouvelles menaces
- La solution doit être capable d'agir comme un proxy inverse et atténuer les attaques en créant de nouvelles requêtes correctement formées lorsque cela est possible ou en ignorant les requêtes lorsqu'elles ne le sont pas
- La solution souhaitée doit être capable d'agir comme un moniteur hors chemin (Out-of-

path monitor) ou comme un Bridge transparent

- La solution souhaitée doit être capable de présenter un message d'erreur personnalisable à l'utilisateur lorsque les demandes d'application Web sont bloquées
- La solution souhaitée doit être capable d'inspecter et de bloquer les requêtes HTTP/SOAP/XML/JSON indésirables/mauvaises/invalides.
- La solution souhaitée doit prendre en charge le filtre de sécurité de la liste autorisée. Le filtre de sécurité de la liste doit permettre de valider que les requêtes HTTP sont approuvées.
- La solution proposée doit disposer de mécanisme de filtre de sécurité Brute Force qui doit assurer la protection contre les attaques Brute Force en créant des règles d'action et en bloquant les adresses IP des attaquants potentiels.
- La solution proposée doit prendre en charge le filtre de sécurité de la base de données. Le filtre de sécurité de la base de données doit permettre de valider les paramètres des requêtes HTTP en détectant les injections de commandes SQL nuisibles.
- La solution souhaitée doit prendre en charge le filtre de sécurité de Upload des fichiers. Le filtre de sécurité de Upload de fichiers doit valider les téléchargements de fichiers et les méthodes d'accès aux fichiers téléchargés approuvées.
- La solution souhaitée doit prendre en charge le filtre de sécurité des paramètres globaux. Le filtre de sécurité des paramètres globaux doit permettre de vérifier que les valeurs des paramètres des requêtes HTTP sont acceptables selon les définitions globales répertoriées.
- La solution souhaitée doit prendre en charge le filtre de sécurité des méthodes HTTP. Le filtre de sécurité des méthodes HTTP doit permettre de valider les méthodes de requête HTTP
- La solution souhaitée doit prendre en charge le filtre de sécurité de logs.
- La solution proposée doit prendre en charge le filtre de sécurité des paramètres. Le filtre de sécurité des paramètres doit permettre de vérifie que les valeurs des paramètres des requêtes HTTP sont acceptables selon les définitions répertoriées.
- La solution souhaitée doit assurer le filtrage de sécurité Path-Blocking. Le filtre de sécurité Path-Blocking doit permettre de valider qu'une requête HTTP est interdite, comme les tentatives non autorisées d'accès à des fichiers et dossiers courants
- La solution proposée doit prendre en charge le filtre de sécurité de réponse sécurisée. Le filtre de sécurité Safe Reply doit permettre de détecter la divulgation et le contenu non autorisé dans les messages de réponse sortants, tels que les numéros de carte de crédit et de sécurité sociale.
- La solution proposée doit prendre en charge le filtre de sécurité de session. Le filtre de sécurité de session doit permettre d'empêcher aux utilisateurs distants de manipuler les informations sur l'état de session et de les soumettre à l'application Web.
- La solution souhaitée doit prendre en charge le filtre de sécurité des vulnérabilités. Le filtre de sécurité des vulnérabilités doit permettre de valider les requêtes HTTP à l'aide de validations basées sur des règles qui détectent diverses menaces de sécurité au niveau de la couche application (basées sur les signatures).
- La solution souhaitée doit prendre en charge le filtre de sécurité des services Web. Le filtre de sécurité des services Web doit permettre de valider que les services et les opérations sont approuvés.
- La solution proposée doit prendre en charge le filtre de sécurité XML. Le filtre de sécurité XML doit permettre de valider le corps XML de la demande postérieure et analyse les valeurs XML encapsulées en paramètres pour les distribuer aux filtres de sécurité suivants pour validation.
- La solution souhaitée doit prendre en charge la reconnaissance des hôtes (hosts) de confiance afin que l'appareil n'apprenne que le trafic légitime.
- La solution proposée doit prendre en charge un contrôle de politique très granulaire basé sur le chemin de l'application (application path)

- La solution proposée doit prendre en charge l'apprentissage d'une application sans intervention manuelle
- Le mode Apprentissage de la solution souhaitée doit etre disponible au minimum pour les filtres de sécurité suivants :
  - Allow List
  - Parametres
  - Base de données
  - Vulnérabilités
  - Database Vulnerability
  - Méthodes http
  - Session
- La solution proposée doit prendre en charge l'inspection de la stratégie installée et active au niveau des Devices. L'inspection de la politique doit etre possible à tout moment.
- La solution souhaitée doit prendre en charge l'augmentation automatique du niveau de protection en fonction de la détection d'une attaque.
- La solution doit disposer des mécanismes capables de modifier dynamiquement le niveau de protection chaque fois qu'une attaque est détectée par l'un des appareils de l'environnement. Ces mécanismes doivent nous permettre d'établir des politiques de sécurité qui déclenchent l'augmentation du niveau de protection.
- La solution proposée doit supporter le suivi des modifications de configuration
- La solution proposée doit prendre en charge l'affinement automatique des filtres de sécurité en fonction du trafic et des données statistiques
- La solution souhaitée doit prendre en charge une interface intuitive avec la possibilité de maintenir des politiques distinctes pour différentes applications
- La solution doit prendre en charge un processus simple pour assouplir sélectivement les règles générées automatiquement afin de réduire ou d'éliminer les faux positifs
- La solution doit prendre en charge un processus simple pour accepter manuellement les faux positifs
- La solution proposée doit prendre en charge la personnalisation des politiques de déni de service
- La solution souhaitée doit prendre en charge la configuration d'hôtes (hosts) approuvés capables d'effectuer des opérations non autorisées par la stratégie, par exemple pour permettre des tests d'intrusion ou un dépannage
- La solution doit prendre en charge différentes méthodes d'authentification telles que SSL, les certificats clients SSL et l'authentification client proxy
- La solution souhaitée doit prendre en charge la surveillance du fonctionnement et des performances de l'appliance.
- La solution souhaitée doit permettre à ce que les alertes et les journaux peuvent être générés et envoyés via Syslog et SMTP.
- La solution souhaitée doit prendre en charge l'envoi d'alertes pour les événements suspects à l'aide d'un e-mail ou d'une SNMP Trap
- La solution souhaitée doit prendre en charge la génération de statistiques de performances et du système
- La solution proposée doit supporter la génération des évènements et rapports par Application, filtre de de sécurité et par filtre de sécurité d'application
- La solution proposée doit prendre en charge la génération des rapports manuellement et automatiquement et des rapports lisibles par l'être humain
- La solution doit supporter au minimum les méthodes des notifications ci-dessous :
  - SNMP
  - SMTP
  - OPSEC ELA
  - ODBC

Le périmètre de la solution doit couvrir au moins 30 applications web.

Le prestataire est tenu d'assurer :

- L'intégration de la solution et la mise application des différents utilitaires
- Le tunning de la solution
- Une session de formation de 5 jours pour les équipes de l'ONDA
  - Le soumissionnaire est tenu a présenter au niveau de l'offre technique :
  - Un Engagement de renouvellement du support auprès de l'éditeur durant la période de Maintenance ;
  - Une attestation de l'éditeur de la solution cible proposée autorisant le soumissionnaire à répondre à cet Appel d'Offres ;

b. AQ 2 : Acquisition et mise d'une solution de Durcissement des configurations

L'acquisition d'une solution de gestion de la configuration des composants du système d'information, Celle-ci aura pour but d'auditer les configurations existantes, de gérer les modifications et de pouvoir automatiser et suivre le niveau de durcissement du parc informatique en temps réel.

Elle est composée, au moins, des modules suivants :

- Module d'audit des configurations
- Module de durcissement
- Module de gestion des patchs sécurité
- Module d'inventaire et suivi des utilitaires installés

Le titulaire doit assurer l'installation, la configuration et le paramétrage de ladite solution ainsi que son intégration dans le système d'information de l'ONDA.

Spécifications techniques :

Architecture

- Le titulaire doit fournir les caractéristiques techniques de l'ensemble des composants de la solution proposée (plateforme matérielle, système d'exploitation, base de données, capacité de stockage, etc.)
- Une solution basée sur une machine virtuelle avec un système d'exploitation renforcé (non Windows) ;
- Une solution capable de s'intégrer avec Active Directory ;
- Une solution admettant le stockage de toutes les données localement (pas de cloud).

La solution proposée doit :

- Fournir une console de gestion centralisée ;
- Garantir la modification des modèles (Template) prédéfinis d'analyse de configurations ;
- Être capable de planifier à l'avance les analyses qui s'exécuteront automatiquement sans Intervention humaine ;
- Prendre en charge le contrôle d'accès basé sur les rôles ;
- Garantir un contrôle d'accès hiérarchique déterminé par le profil de l'utilisateur et les niveaux de privilège ;
- Permettre d'accorder différents niveaux de privilèges pour chaque utilisateur de la solution.
- Limiter l'impact sur la bande passante ;
- Eviter la perturbation des services ou des équipements lors de l'audit ;
- Permettre une gestion centralisée des configurations ;
- Produire des rapports automatiques et centralisés à partir d'analyses distribuées.

Configuration et Conformité

La solution cible doit :

- Permettre d'affecter des actifs à des exigences spécifiques en matière de politiques de Sécurité ;
- Pouvoir déterminer si les systèmes analysés sont conformes aux politiques de l'ONDA et de réglementation tels que DGSSI, PCI, ANSSI, GDSSI, HIPAA ;
- Fournir des modèles de conformité prédéfinis ;
- Supporter la modification des contrôles de conformité ;
- Être capable de détecter les vulnérabilités relatives à des défauts ou erreurs de configuration ;
- Identifier le niveau de règles de sécurité ;
- Toute communication entre les composants de la solution doit être chiffres.
- Permettre d'effectuer une analyse des correctifs de n'importe quel système d'exploitation Linux, REDHAT, UNIX, AIX ou Windows.
- Permettre de suivre la mise en place des patchs sécurité
- Permettre l'audit et durcissement des bases de données (ORACLE, SQL SERVER …)
- Permettre l'audit et durcissement des serveurs web (TOMCAT, JBOSS, NGINX…)
- La solution doit permettre de créer des groupes dynamiques et des groupes statiques, les groupes dynamiques doivent être rempli automatiquement par les ordinateurs ou équipement du même type selon le filtrage mis en place
- Permettre l'analyse approfondie des contrôleurs de domaine Active Directory
- Les groupes dynamiques des assets doit permettre d'ajouter ou/et supprimer automatiquement une adresse IP qui ne respecte plus les critères du filtre.
- La solution doit disposer de plusieurs modèles de risk incluant real risk context qui permettra de s'adapter selon la criticité des assets et la zone scanner, la solution doit être capable de fournir des modèles de risk qui s'adapterons a la politique de gestion de risk propre à l'ONDA
- La solution doit permettre d'adapter et tuner les templates de scans par assets ou groupe d'assets afin d'avoir de meilleurs résultats.

Administration et Déploiement

- La solution doit supporter le regroupement des actifs selon leur fonction métier.
- Elle doit fournir la possibilité de sauvegarder et de restaurer la configuration système.
- Le soumissionnaire est tenu de fournir le guide de gestion des utilisateurs ainsi que les manuels d'administration de la solution.

Reporting

Le soumissionnaire doit fournir une solution permettant :

- La production des modèles de rapports prédéfinis ;
- La personnalisation des modèles de ces rapports ;
- La génération de rapports de remédiation ;
- La comparaison des résultats d'analyse des configurations dans le temps.
- La prise en charge des navigateurs web les plus utilisés (internet explorer, Firefox, chrome, etc.) pour l'accès aux rapports générés
- De supporter la génération et la distribution automatisées des rapports par courrier électronique.
- La création des filtres de rapport par différents critères : OS, serveurs, groupe OS, application, protocoles, host.
- L'envoi par e-mail des rapports à haut risque.
- L'exportation des rapports d'analyse aux formats PDF, HTML, CSV et XML

Gestion d'accès

Le soumissionnaire est tenu de proposer une solution permettant de :

- Gérer les utilisateurs de manière détaillée et granulaire ;

- Créer des utilisateurs et groupes d'utilisateurs avec un niveau varié des droits d'accès et des privilèges ;
- Gérer les droits d'accès à base de rôle ;
- Tracer toutes les activités effectuées par les utilisateurs de la solution ;
- Autoriser l'association de la relation {Rôle, Privilège}, et définit les privilèges accordés à chaque utilisateur/groupe.

Spécifications fonctionnelles de la solution

Le dimensionnement de la solution doit supporter au moins les éléments suivants :

Durcissement des configurations	Nombre
Nombre Serveur Windows	160
Nombre serveur UNIX	20
Nombre Base de données	60
Nombre Serveur Web	15

Module audit de configuration

Le module doit permettre l'audit et suivi en temps réel de la configuration des composants selon les guides de gestion des configurations de la DGSSI et les bonnes pratiques en terme de gestion des configurations (CIS, NIST, SWIFT CSP, …..).

A ce titre il doit proposer les fonctionnalités attendues par l'ONDA. Cette liste peut être amendée ou complétée en fonction des capacités de la solution.

Audit et contrôle

- Audit des niveaux de configuration
- Audit des systèmes
- Le contrôle/la vérification de la conformité des serveurs du SI par rapport aux guides de configuration OS Windows, AIX et Linux,
- Le contrôle/la vérification de la conformité des serveurs de base de données par rapport aux guides de configuration (MS SQL, ORACLE, MYSQL),
- Le contrôle/la vérification de la conformité des serveurs WEB par rapport aux guides de configuration (TOMCAT, JBOSS, XAMPP, IIS) ;
- S'intégrer avec les plateformes DEVSECOPS

Détection

- Détection des patchs manquants
- Détection des utilitaires installées (suivi de l'activité)
- Automatiser les contrôles de conformités
- Dégradation du niveau de sécurité d'un actif

La solution devra auditer les différents composants du périmètre et vérifier leur conformité par rapport aux guides de durcissement en vigueur en termes de protection des données, contrôle d'accès, traçabilité, paramètres de sécurité systèmes, etc.

La solution doit permettre le choix des politiques d'audit avec la possibilité d'auditer a base d'une politique appropriée de l'ONDA.

Maintien et monitoring

- Réaliser un monitoring continu des configurations
- Permettre la mise en œuvre de taches automatiques (ex: planification des audits …)

- Avoir un tableau de bord pour mesurer et suivre les indicateurs de santé de la configuration

Module durcissement des configurations

Afin de pouvoir automatiser les taches de durcissement et l'implémentation de la politique de durcissement et les guides de durcissement, la solution doit prendre en charge les fonctions citées ci-dessus sur les plateformes cibles suivantes :

- Serveurs Linux
- Serveurs Windows
- Endpoint
- Serveurs AIX
- Serveurs REDHAT
- Serveurs web (Tomact, IIS, XAMPP)
- Serveurs Base de données (MYSQL, ORACLE, MSSQL…)

La solution doit permettre de :

- Définir des politiques de durcissement
- Mise en œuvre de la stratégie de durcissement
- Fournir des modèles (Template) prédéfinis d'analyse des configuration et durcissement ;
- L'analyse régulière des mises à jour les plus récentes de chacun des composants du système d'exploitation et de les appliquer

Installation, Configuration et mise en œuvre

Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution, ainsi que le planning de réalisation.

Le prestataire doit accompagner l'ONDA pour l'élaboration des guides de durcissement des composants.

Ces prestations doivent inclure l'ingénierie, l'installation, la configuration, le paramétrage, l'intégration et la mise en service de la solution de sécurité proposée.

Le prestataire doit réaliser tout essai qu'il jugera nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité.

- Le titulaire assurera ainsi la mise en place de l'architecture technique cible et la mise en service des dispositifs de la solution.
- La prestation de service demandée est résumée dans les points suivants :
- Élaborer l'architecture technique de la plateforme, et l'ingénierie d'interconnexion avec l'existant.
- Assurer le transfert de compétences sur la solution.

Installation et Configuration :

- Installation, paramétrage et optimisation de la partie serveur ;
- Installation et paramétrage des agents à déployer sur les serveurs ;
- Mise en place et paramétrage de la partie gestion des droits ;
- Mise en place et paramétrage de la partie reporting ;
- Mise en place et paramétrage de la partie délégation des droits ;

Formation

Le prestataire est tenu d'assurer une session de formation au profit des équipes de l'ONDA pour une durée de 3 jours

Le soumissionnaire est tenu à présenter au niveau de l'offre technique :

- Un Engagement de renouvellement du support auprès de l'éditeur durant la période de

Maintenance.
- Une attestation de l'éditeur de la solution cible proposée autorisant le soumissionnaire à répondre à cet Appel d'Offres

c. AQ3 : Mise en place des solutions NAC (Network Access Contrôle) au niveau des sites de l'ONDA

L'ONDA souhaite mettre en place un contrôle des accès réseaux au niveau des différents sites à travers solution NAC de nouvelle génération qui identifie et évalue de manière dynamique les terminaux et les applications du réseau dès qu'ils se connectent au réseau du client L'ONDA avec ou sans agent. La solution proposée doit déterminer rapidement l'utilisateur, le propriétaire et le système d'exploitation, ainsi que la configuration de l'appareil, les logiciels, les services, l'état des correctifs et la présence d'agents de sécurité. Dans le même temps, la solution NAC de nouvelle génération proposée devrait fournir une correction, un contrôle et une surveillance continue de ces dispositifs. Les actions de contrôle doivent tenir compte de l'infrastructure réseau existante et de la conception du réseau afin de minimiser les exigences de déploiement.

La solution NAC de nouvelle génération proposée doit effectuer les actions ci-dessus sur les terminaux BYOD (Bring Your Own Device) et sur les appareils non traditionnels, sans nécessiter d'agents logiciels ni de connaissances préalables sur les appareils.

La solution proposée doit être rapidement déployée dans notre environnement existant et ne doit pas nécessiter de modifications et de mises à niveau majeures de l'infrastructure.

Le dimensionnement de la solution doit supporter au moins les éléments suivants :

NAC périmètre	Nombre des postes DATA
Site 1 siège DSI	1500
Site 2	150
Site 3	150
Site 4	60
Site 5	60
Site 6	70
Site 7	50
Site 8	50
Site 9	20
Site 10	20
Site 11	20
Site 12	20
Site 13	20
Site 14	20
Site 15	20
Site 16	20
Site 17	20
Site 18	20
Site 19	20
Site 20	20
Site 21	20
Site 22	20
Site 23	20

Site 24	20

NB : La solution doit être évolutif doit supporter 3000 Endpoint extensible à 6000

La solution proposée doit améliorer la visibilité des terminaux et fournir des informations basées sur des politiques, l'application, l'atténuation des risques, la correction et la surveillance en temps réel de tous les terminaux IP connectés. La plate-forme de sécurité proposée doit prendre en charge les éléments suivants :

- Surveiller l'état des terminaux sur le réseau en temps réel. La plate-forme de sécurité NG-NAC doit prendre en charge l'inventaire et suivre l'état de sécurité de tous les types d'appareils lorsqu'ils demandent l'accès et s'exécutent sur les réseaux d'entreprise. Il doit également identifier et évaluer les utilisateurs, les appareils, les systèmes et les applications du réseau pour fournir des renseignements opérationnels et permettre d'atténuer les problèmes de sécurité.
- Appliquer des politiques granulaires pour le contrôle d'accès et la conformité des terminaux. La plate-forme de sécurité NG-NAC doit prendre en charge la capture de toutes les données des terminaux, afin de donner aux opérations de sécurité les informations dont elles ont besoin pour comprendre leur risque, prendre des décisions intelligentes et prendre des mesures en fonction d'un large ensemble d'attributs tels que : type d'appareil, utilisateur, l'emplacement, l'état d'authentification, l'exposition à la sécurité ou d'autres considérations commerciales. Il devrait offrir une gestion des invités et identifier et supprimer automatiquement les appareils malveillants et les applications non autorisées.
- Traiter les opérations de sécurité avec une correction automatisée de la sécurité du réseau. La plate-forme de sécurité NG-NAC doit être en mesure de réagir aux violations et aux menaces de sécurité en activant des actions automatisées basées sur des politiques. Les réponses simples peuvent inclure l'alerte, l'enregistrement et la notification au service informatique ou à l'utilisateur d'un problème de sécurité. Des réponses plus fortes peuvent être effectuées au niveau de l'application du réseau, comme autoriser, limiter ou refuser l'accès aux ressources réseau. Il doit également proposer une correction au niveau de l'appareil, comme l'installation d'un correctif, la modification d'un paramètre de sécurité ou la fermeture d'une application. Cela peut permettre les changements souhaités dans le comportement de l'utilisateur final, réduire le temps nécessaire à la découverte et à la réponse, et minimiser les dommages potentiels associés aux cyberattaques.
- Agir en tant que hub d'intégration pour partager des données avec d'autres outils de cybersécurité. La plate-forme de sécurité NG-NAC doit appliquer une approche ouverte et normalisée pour permettre à la plate-forme d'échanger des données sur les terminaux et d'améliorer le contexte de contrôle avec d'autres outils de sécurité tels que les systèmes SIEM, les renseignements sur les menaces, le MDM et les scanners de vulnérabilité. Ce partage de données nous aiderait à renforcer le réseau, à enquêter et à identifier les problèmes, et à accélérer les tâches de remédiation.

Exigences fonctionnelles

Les caractéristiques fonctionnelles ci-dessous doivent être prises en charge par la solution NAC de nouvelle génération proposée :

1. Accompagnement hétérogène. Il devrait fonctionner avec l'infrastructure réseau, les systèmes d'exploitation, les logiciels de point de terminaison et les solutions de sécurité tierces populaires sans dépendre de 802.1x - En fait, les ACL basées sur les rôles devront être provisionnées dynamiquement sur les ports d'accès en fonction du profil de l'appareil et de l'appartenance au domaine AD.

2. Sans agent –La solution doit être opérationnelle conviviale - donc prendre en charge le profilage sans agent, au cas où des ordinateurs Windows non-domaine seraient trouvés dans les réseaux de production, nous devons être en mesure de les mettre en quarantaine (même s'ils sont configurés avec des adresses IP statiques) - jusqu'à ce qu'une enquête plus approfondie soit effectuée - sur un seul VLAN.
3. Visibilité complète. Voir tous les appareils qui se connectent au réseau, c'est-à-dire les ordinateurs de bureau, les ordinateurs portables, les téléphones intelligents, les tablettes, les appareils IOT (projecteurs, caméras IP, appareils HVAC.).
4. Contrôle automatisé. Prend en charge l'automatisation avec une vaste gamme d'actions, telles que :
   a. Accorder, refuser ou limiter l'accès au réseau en fonction de la position de l'appareil et des politiques de sécurité
   b. Mettez en quarantaine et corrigez les terminaux malveillants/à haut risque
   c. Application flexible des politiques. Appliquez le contrôle d'accès au réseau, la conformité des terminaux et la sécurité des appareils mobiles.
5. Productivité. Accordez un accès réseau approprié aux personnes et aux appareils, sans intervention intrusive ni implication du personnel
6. Fiabilité. Améliorer la stabilité du réseau en identifiant et en supprimant les infrastructures malveillantes
7. Conformité. Identifiez automatiquement les violations de politique, corrigez les défaillances des terminaux et mesurez le respect des obligations de conformité.
8. Orchestration- La solution doit prendre en charge de larges capacités d'intégration avec les principaux NGFW, ATD, VA, EPP / EDR, EMM, Threat Intelligence en plus des principaux fournisseurs SIEM

Appareil de gestion d'entreprise/virtuel

	Caractéristiques
1	La solution doit prendre en charge la gestion centralisée avec une licence centralisée
2	La solution proposée doit prendre en charge la gestion d'entreprise via une machine virtuelle ou une appliance pour gérer toutes les appliances à partir d'une seule console d'administration lorsque plusieurs appliances/machines virtuelles sont utilisées pour couvrir la solution
3	La solution doit prendre en charge la haute disponibilité pour la gestion d'entreprise
4	La solution doit prendre en charge le tableau de bord interactif pour la visibilité et l'état de conformité
5	La solution doit prendre en charge le tableau de bord de l'inventaire des actifs
6	La solution doit prendre en charge jusqu'à 30 appliances de point de terminaison/gestion de la configuration virtuelle

Appareils de contrôle des points finaux/Virtuel

	Caractéristiques
1	La solution proposée doit prendre en charge l'inspection approfondie des paquets sans nécessiter l'intégration d'un tiers/d'un autre fournisseur.
2	La solution proposée doit être capable de prendre en charge le périmètre de l'ONDA
3	La solution proposée doit être capable de gérer jusqu'à 500 appareils de couche 2 / couche 3 en mode non 802.1X.
4	La solution proposée doit être hautement disponible et évolutive.
5	La solution proposée doit être évolutive pour une expansion future sans nécessiter de modifications majeures de l'architecture.
6	La solution proposée doit prendre en charge la surveillance et l'évaluation continues des terminaux lorsqu'ils sont connectés à l'infrastructure réseau (réévaluation périodique)
7	La solution proposée doit prendre en charge les systèmes d'exploitation Windows, Linux et Mac OS et doit prendre en charge les anciens systèmes d'exploitation Windows.
8	La solution proposée doit être capable de bloquer l'accès des terminaux qui sont connectés sur un réseau non géré (c'est-à-dire un commutateur non géré).
9	La solution proposée doit prendre en charge la détection d'usurpation d'identité MAC lorsque l'appareil est connecté au même commutateur ou à un commutateur différent du réseau
10	La solution proposée doit prendre en charge la détection d'usurpation d'identité MAC en vérifiant les changements de caractère du périphérique (nom de domaine DHCP, nom d'hôte DHCP, classe de fournisseur DHCP, empreinte digitale de requête DHCP ou fonctionnalité réseau,
11	La solution proposée doit être capable d'identifier les appareils IOT tels que : caméras IP, VOIP, projecteurs, appareils CVC, etc.
12	Le système doit avoir plusieurs méthodes de découverte actives et passives.
13	Il doit prendre en charge l'authentification de l'utilisateur et de la machine sans aucune configuration supplémentaire
14	Doit prendre en charge le profilage des appareils sans client en fonction d'une empreinte DHCP, d'une analyse NMAP, de l'OUI du fournisseur, de l'emplacement, des ports ouverts et de l'existence de l'agent persistant
15	La solution proposée doit prendre en charge l'évaluation des informations d'identification IoT (informations d'identification par défaut, communautés SNMP par défaut, informations d'identification d'usine par défaut, etc.)

16	La solution proposée doit prendre en charge la vérification passive et active des vulnérabilités bien connues et des IOC
17	La solution fournie doit fournir un nombre illimité de licences d'appliances virtuelles pour couvrir le nombre total de points de terminaison IP demandés (nombre de points de terminaison).
18	La solution proposée doit prendre en charge les interfaces cuivre et fibre (1G/10G).
19	La solution proposée doit pouvoir s'intégrer à une grande variété de fournisseurs de commutation réseau tels que Cisco, Juniper, Brocade / Foundry, etc.
20	La solution proposée doit avoir une gestion virtuelle ou une appliance dédiée pour gérer toutes les appliances à partir d'une seule console d'administration.
21	L'appliance/virtuelle de la solution proposée doit être déployée dans un centre de données centralisé.
22	La solution proposée ne devrait nécessiter aucune modification de l'architecture du réseau
23	La solution proposée doit être déployée sans nécessiter 802.1X pour les fonctionnalités de contrôle d'accès
24	La solution proposée doit prendre en charge les techniques d'empreintes digitales passives et actives pour les terminaux traditionnels et les appareils IoT industriels.
25	La solution proposée ne doit pas nécessiter qu'un agent effectue le profilage des points finaux, l'évaluation de la posture et la définition des références pour les fonctionnalités complètes de la solution NAC (pour les appareils gérés). L'agent peut être utilisé pour les points de terminaison Windows membres AD gérés.
26	La solution proposée doit être capable d'identifier les appareils IOT tels que : caméras IP, VOIP, projecteurs, appareils HVAC…
27	La solution proposée doit être capable de fournir une surveillance post-connexion sans agent.
28	La solution proposée doit fournir une visibilité et un contrôle sur les machines virtuelles du centre de données et son infrastructure virtualisée
29	La solution proposée doit permettre aux administrateurs d'examiner les événements, d'effectuer des recherches et d'exécuter des rapports à partir d'une interface utilisateur Web.
30	La solution proposée doit prendre en charge la journalisation des événements via la gravité
31	La solution proposée doit prendre en charge le contrôle d'accès basé sur les rôles pour la gestion

32	Notification d'alerte d'assistance propose
33	La solution proposée doit prendre en charge la génération de rapports au format csv, xls ou pdf
34	La solution proposée doit prendre en charge la création de rapports personnalisés
35	La solution proposée doit prendre en charge la notification du service d'assistance
36	La solution proposée doit prendre en charge la restriction d'accès basée sur le chiffrement
37	La solution proposée doit prendre en charge la restriction d'accès basée sur les correctifs
38	La solution proposée doit prendre en charge la restriction d'accès basée sur AV
39	La solution proposée doit prendre en charge la restriction d'accès basée sur le périphérique géré
40	La solution proposée doit prendre en charge la restriction d'accès basée sur le compte AD/LDAP
41	Expliquez comment la solution proposée peut empêcher les stations terminales ne respectant pas la politique d'accéder au réseau et les alternatives pour mettre en quarantaine et/ou réparer les ordinateurs non conformes.
42	La méthode de quarantaine de solution proposée ne doit pas reposer sur du matériel ou des logiciels spécialisés.
43	La solution proposée doit prendre en charge la restriction VLAN, le bloc de port de commutateur, l'ACL dynamique, les ACL basées sur les ports
44	La solution proposée doit prendre en charge le pare-feu virtuel basé sur une étendue passive.
45	La solution proposée doit prendre en charge la vérification avant et après l'admission, la revérification de la politique
46	La solution proposée doit prendre en charge les capacités de conformité et de correction
47	La solution proposée doit prendre en charge les capacités de gestion des invités pour pouvoir configurer rapidement et facilement un compte invité sans engager le personnel informatique et sans nécessiter de licence supplémentaire
48	Décrivez les options de configuration de la politique de solution proposées : celles configurées prêtes à l'emploi (meilleures pratiques) et la flexibilité dont dispose l'État pour personnaliser la solution (méthodes de vérification de l'état, étendue des options de vérification de l'état).

49	La solution proposée doit prendre en charge la détection automatique de nouveaux terminaux connectés au réseau. Veuillez décrire comment cela peut être fait avec la solution proposée.
50	La solution proposée devrait être un câble d'identification des hôtes virtuels par rapport aux hôtes physiques
51	La solution doit être en mesure d'identifier le fournisseur de la carte réseau des terminaux
52	La solution doit être en mesure d'identifier le nom du commutateur et le port du commutateur auquel le point de terminaison est connecté
53	La solution proposée doit être en mesure d'identifier l'utilisateur, l'adresse e-mail et l'adresse IP des appareils gérés sans nécessiter d'agent grâce à l'intégration avec le serveur LDAP existant.
54	La solution proposée doit être en mesure d'identifier sur la gestion la présence/l'absence (sans nécessiter d'agent) : 1- Services Windows Processus à 2 fenêtres 3 ports ouverts 4-Appareils externes
55	La solution doit être capable d'identifier les applications en cours d'exécution sur les périphériques gérés sans nécessiter d'agent.
56	La solution doit être en mesure d'identifier et de classer le système d'exploitation et les niveaux de correctifs installés sur les appareils gérés sans nécessiter d'agent.
57	La solution doit s'intégrer aux principaux fournisseurs SIEM
58	La solution proposée doit prendre en charge les serveurs d'annuaire d'utilisateurs suivants : • Microsoft Active Directory • Novell eDirectory. • Serveur d'annuaire Sun. • IBM Lotus Notes. • Ouvrez le serveur LDAP. • Serveur de protocole Radius
59	La solution proposée doit prendre en charge le système d'exploitation Windows suivant : • Windows 11 v21H2 • Windows 10 (v1809, v1903, v1909, v2004, v20H2, v21H1) • Windows 8 et 8.1 • Windows 7 • Windows Vista

60	La solution proposée doit prendre en charge le système d'exploitation Windows Server suivant : • Serveur Windows (v21H2, v20H2, v2004) • Serveur Windows 2022 • Serveur Windows 2019 • Serveur Windows 2016 • Serveur Windows 2012 • Serveur Windows 2008 • Serveur Windows 2003
61	La solution proposée doit prendre en charge le système d'exploitation MAC suivant : • OS X 10.6 (léopard des neiges) • OS X 10.7 (Lion) • OS X 10.8 (Mountain Lion) • OS X 10.9 (Mavericks) • OS X 10.10 (Yosemite) • OS X 10.11 (El Capitan) • Mac OS 10.12.x (Sierra) • Mac OS 10.13.x (High Sierra) • Mac OS 10.14.x (Mojave) • Mac OS 10.15.x (Catalina) • Mac OS 11.x (Big Sur) • Mac OS 12.x (Monterey)
62	La solution proposée doit prendre en charge le système d'exploitation Linux suivant : • CentOS • DebianName • Feutre • Kali • menthe • Red Hat Enterprise Linux • Bureau d'entreprise Red Hat • chapeau rouge • Ouvrir Suse • Suse Entreprise • Ubuntu • IGEL
63	La solution proposée doit prendre en charge l'évaluation de la posture des terminaux Linux tout en fournissant un inventaire des applications, des processus et des ports ouverts sur un terminal. En outre, la solution doit inclure des actions de correction telles que l'arrêt des processus, l'exécution de scripts, la définition de clés de registre ou la désactivation des adaptateurs de périphérique à double hébergement.
64	La solution proposée doit prendre en charge l'intégration avec Leading Vulnerability Management, la solution SIEM et les solutions ATD. La solution NAC proposée doit être capable de prendre des mesures automatiques en fonction

	des messages reçus de la solution SIEM (ACL de point de terminaison, ACL basées sur les ports, bloc de port de commutateur, pare-feu virtuel).
65	La solution proposée doit prendre en charge l'intégration avec SCCM sans nécessiter la création de requêtes SQL (l'intégration doit être simple et prête à l'emploi)
66	La solution proposée doit prendre en charge l'évaluation de la posture des terminaux Linux tout en fournissant un inventaire des applications, des processus et des ports ouverts sur un terminal. En outre, la solution doit inclure des actions de correction telles que l'arrêt des processus, l'exécution de scripts, la définition de clés de registre ou la désactivation des adaptateurs de périphérique à double hébergement.
67	La solution proposée doit s'intégrer à LDAP/AD

Installation, Configuration et mise en œuvre

Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution, ainsi que le planning de réalisation.

Le prestataire doit accompagner l'ONDA pour l'élaboration des guides de durcissement des composants.

Ces prestations doivent inclure l'ingénierie, l'installation, la configuration, le paramétrage, l'intégration et la mise en service de la solution de sécurité proposée.

Le prestataire doit réaliser tout essai qu'il jugera nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité.

- Le titulaire assurera ainsi la mise en place de l'architecture technique cible et la mise en service des dispositifs de la solution au niveau des différents site (territoire nationale).
- La prestation de service demandée est résumée dans les points suivants :
- Élaborer l'architecture technique de la plateforme, et l'ingénierie d'interconnexion avec l'existant.
- Assurer le transfert de compétences sur la solution.

Installation et Configuration :

- Installation, paramétrage et optimisation de la partie serveur ;
- Installation et paramétrage des agents à déployer sur les serveurs ;
- Mise en place et paramétrage de la partie gestion des droits ;
- Mise en place et paramétrage de la partie reporting ;
- Mise en place et paramétrage de la partie délégation des droits ;

Formation

Le prestataire est tenu d'assurer une session de formation officielle au profit des équipes (7 personnes) de l'ONDA pour une durée de 5 jours

Le soumissionnaire est tenu à présenter au niveau de l'offre technique :

- Un Engagement de renouvellement du support auprès de l'éditeur durant la période de maintenance ;
- Une attestation de l'éditeur de la solution cible proposée autorisant le soumissionnaire à répondre à cet Appel d'Offres

d. AQ4 : Traçabilité VPN/Concentrateur VPN

1. La solution proposée doit être leader du dernier classement Gartner Magic Quadrant et

Forrester Wave pour les outils UEM (Unified Endpoint Management).

2. La solution proposée doit être installée On-Premise. Toute la plateforme (gestion et administration) doit être installée dans nos installations. Le soumissionnaire est tenu de mettre à notre disposition tous les prérequis nécessaires.
3. La solution proposée doit nous permettre d'utiliser la même Appliance comme une solution de Network Access Control par un simple changement de licence
4. La solution proposée ne doit en aucun cas être incluse dans un Firewall. Elle ne doit en aucun cas dépendre d'une configuration des tunnels VPN ou autre configuration ZTNA au niveau des Firewalls. La configuration des règles des accès et des VPN doivent être incluse obligatoirement dans la même plateforme.
5. La solution souhaitée doit être disponible sous le format ci-dessous :
   - Appliance physique
   - Appliance Virtuelle (VMware, KVM, Hyper-V)
   - Cloud (Azure, AWS)
6. La solution doit offrir au minimum les 3 méthodes de déploiement ci-après :
   - Core (Web) Access : Cette méthode doit permettre l'acces via un navigateur WEB et ne doit nécessiter aucun client.
   - Application Layer Access : Cette méthode doit fournir l'accès à partir d'un client léger SAM (Secure Application Manager). Le SAM doit fournir un accès à distance à l'aide de noms d'applications et de destinations et ne doit nécessiter aucun adaptateur virtuel ou d'adresse IP virtuelle sur le terminal.
   - Network Layer Access : Cette méthode doit offrir une expérience utilisateur VPN, servant de mécanisme d'accès à distance supplémentaire aux ressources de l'entreprise.
7. La méthode Core (Web) Access supporté par la solution doit offrir des accès sécurisés ci-après :
   - L'accès sécurisé aux ressources et applications web de l'entreprise
   - L'accès Web sécurisé aux partages des fichiers Windows et Network File System
   - L'accès sécurisé aux ressources RDP, Telnet et SSH à l'aide de HTML5
   - L'accès sécurisé au Terminal Services (Citrix et Windows)
   - L'accès sécurisé au Virtual Desktop Infrastructure (Citrix XenDesktop et VMware View)
8. La méthode Application Layer Access supporté par la solution doit offrir des accès sécurisés ci-après :
   - Accès fourni pour des applications spécifiques seulement
     - ✓ Avec Définition par nom d'application, port ou les deux
     - ✓ Avec Définition par destination host ou réseau
   - La méthode Application Layer Access doit prendre en charge de multiplateformes ci-dessous :
     - ✓ Windows
     - ✓ Mac (JSAM only)
     - ✓ Linux (JSAM only)
9. La méthode Network Layer Access supporté par la solution doit offrir les fonctionnalités minimales ci-après :
   - Support d'un adaptateur Ethernet virtuel
   - Dual mode de transport - ESP ou SSL
   - Prises en charge des applications basées sur UDP et des connexions lancées par le serveur
   - Fonctionne sur Windows, Mac et Linux
   - Méthode la moins granulaire pour sécuriser l'accès aux ressources (fournit l'accès IP aux ressources, facilitant la prise en charge des applications et serveurs personnalisés).
10. Le client VPN proposé par la solution en cas de configuration en mode Network Layer Access doit être le même que pour la solution Network Access Control. Il doit faire la

différence sans changement de configuration selon que l'Appliance est configurée étant que NAC ou Concentrateur VPN

11. La solution souhaitée doit permettre la configuration VPN en mode tunneling. Cette configuration doit disposer des fonctionnalités ci-dessous au minimum :
    - Network Layer remote access
        - ✓ 2 modes: high performance (ESP) ou high availability (SSL)
        - ✓ Traverses proxies et firewalls
        - ✓ Client
        - ✓ Network Connect
    - GINA integration avec Network Connect
    - Supporte Full-tunnel ou split-tunnel

12. La solution souhaitée doit disposer d'un logiciel client multiservice qui fournit les connexions nécessaires pour des services d'accès et de contrôle d'accès sécurisés. Ce client doit assurer les fonctions ci-dessous :
    - Une interface simplifiée et centralisée
    - SAM application access
    - VPN tunneling
    - Assurer la conformité des endpoints
    - Collaboration
    - Location awareness
    - Always-On
        - ✓ Machine and/or User
    - Lock Down
13. Le client VPN de la solution proposée doit disposer de la fonction de détection d'emplacement qui permet de se connecter automatiquement au bon service en fonction de son emplacement.
14. La fonction Location awareness doit fournir un accès dynamique aux utilisateurs. Cet accès doit être basé sur les règles qui doivent être configurées en se basant sur les critères minimums ci-après :
    - DNS server
    - Resolve address
    - Endpoint address
15. La solution souhaitée doit etre basée sur Trusted Network Communications (TNC) pour fournir une solution complète permettant d'évaluer la fiabilité des Endpoints souhaitant se connecter au VPN.
16. Les composants de Trusted Network Communications (TNC) de la solution souhaitée doit permettre de sécuriser les systèmes utilisateur à l'intérieur et à l'extérieur de réseau avant de les autoriser à se connecter à l'Appliance VPN
17. L'architecture Trusted Network Communications (TNC) doit s'appuyer sur des normes et technologies établies, indépendantes des fournisseurs, telles que :
    - 802.1X, RADIUS
    - La sécurité IP (IPsec)
    - Le protocole d'authentification extensible (EAP)
    - Transport Layer Security (TLS)/Secure Sockets Layer (SSL).
18. Les composants de Trusted Network Communications (TNC) de la solution souhaitée doivent être formés de :
    - Host Checker
    - Cache Cleaner
19. Le Host Checker doit être un composant natif de la solution proposée et doit effectuer des vérifications des Endpoints sur les hôtes qui se connectent à la solution proposée.
20. Pour les hôtes exécutant Windows, Macintosh, Linux et Solaris, Le Host Checker doit assurer

que les processus, fichiers ou ports spécifiés sont conformes à nos spécifications avant d'autoriser un utilisateur à accéder à un domaine, un rôle ou une stratégie de ressources.

21. La politique de vérification des Host doit comprendre au minimum les critères ci-dessous :
    - Antivirus : qui permet de créer une règle qui vérifie le software antivirus qu'on spécifie et permet de spécifier les options de remédiation.
    - Firewall : qui permet de créer une règle qui vérifie le software Firewall qu'on spécifie et permet de spécifier les options de remédiation.
    - Malware : qui permet de créer une règle qui vérifie le software protection malware qu'on spécifie.
    - Spyware : qui permet de créer une règle qui vérifie le software de protection spyware protection que l'on spécifie
    - OS Checks : qui permet de créer une règle qui vérifie le Windows operating system et le minimum service pack versions que l'on spécifie
22. Le Host Checker doit supporter au minimum les plateformes ci-après :
    - Windows
    - Mac
    - Linux
    - Solaris
23. Le Host Checker doit être également disponible sur certaines plates-formes mobiles telles que :
    - Android
    - iOS.
24. Le Host Checker doit vérifier la présence ou absence des éléments ci-après:
    - Processus
    - Fichiers
    - Ports
    - Registry entries pour Windows
25. Pour chaque stratégie Host Checker, la solution souhaitée doit donner la possibilité de configurer deux types d'actions correctives ci-dessous :
    - User-driven : à l'aide d'instructions personnalisées et de chaînes de raison, nous devons être capable d'informer l'utilisateur de l'échec de la stratégie et de la manière de rendre son ordinateur conforme. L'utilisateur doit prendre des mesures pour réévaluer avec succès la stratégie ayant échoué.
    - Automatique (piloté par le système) : La solution doit permettre de configurer Host Checker pour corriger automatiquement l'ordinateur de l'utilisateur. Par exemple, lorsque la stratégie initiale échoue, nous devons être capable d'arrêter des processus ou supprimer des fichiers
26. En plus de l'application native Host Checker, la solution proposée doit prendre en charge une intégration étroite de Host Checker avec de nombreuses applications tierces (pour Windows et Mac).
27. Si l'ordinateur de l'utilisateur ne répond à aucune des exigences de Host Checker, La solution souhaitée doit afficher une page de correction avec les instructions et des liens vers des ressources pour aider l'utilisateur à mettre son ordinateur en conformité.
28. Le Cache Cleaner doit être un composant natif de la solution proposée et doit permettre de supprimer les données résiduelles, telles que les fichiers temporaires ou les caches d'applications, de la machine d'un utilisateur après une session.
29. Le cache Cleaner doit inclure au minimum les fonctions ci-après :
    - Clearing complet du cache, des cookies, des fichiers temporaires ou des caches d'applications
    - Clearing basé sur l'hôte source, le domaine, le fichier et le dossier
    - Clearing de noms d'utilisateur, mots de passe et adresses Web dans les navigateurs
30. En plus des composants TNC, La solution proposée doit être capable d'appliquer d'autres

éléments des Endpoints tels que :
- L'adresse IP source
- Le type de navigateur
- L'utilisation du certificat

31. Le client VPN de la solution souhaitée doit remplir un minimum des fonctions ci-dessous :
    - Secure Access Service
    - Access Control Service
        - ✓ Layer 3 and 802.1X enforcement
    - Dynamic VPNs for Juniper Networks SRX Series devices
        - ✓ Legacy functionality
    - Compliance and remediation
32. Le client VPN de la solution proposée doit supporter au minimum les plateformes ci-après :
    - Windows
    - Mac
    - Linux
    - Apple iOS
    - Google Android
    - Chrome OS
    - Windows mobile devices
33. Le client de la solution souhaitée est disponible sous forme d'application pour les appareils mobiles et doit permettre :
    - Remote L3 VPN capabilities
    - Per-app VPN
    - Host Checker
    - Collaboration
34. La solution souhaitée doit disposer des fonctionnalités
    - Always-on Client: qui doit permettre d'empêcher les utilisateurs finaux de contourner les connexions Pulse Secure. Cette option doit désactiver tous les paramètres de configuration qui permettent à l'utilisateur final de désactiver ou de supprimer les connexions, services ou logiciels
    - Secure.VPN only access
    - Allow saving logon information
    - Allow user connections: qui peuvent etre ajoutées par l'utilisateur
    - Display Splash Screen: Contrôle si l'écran de démarrage s'affiche au démarrage de Client
    - Dynamic certificate trust: Détermine si les utilisateurs peuvent choisir de faire confiance aux certificats inconnus..
    - Dynamic connections
    - EAP Fragment Size
    - Enable captive portal detection: qui doit permettre de tenter de détecter la présence d'un point d'accès de portail captif..
    - Enable embedded browser for captive portal
    - Enable embedded browser for authentication
    - FIPS mode enabled: qui doit permettre de déploiyer le client avec Federal Information Processing Standard activé.
    - Wireless suppression
    - Prevent caching smart card PIN : qui garantit que la valeur du code PIN de la carte à puce n'est pas mise en cache par le processus client.
35. Le client VPN de la solution proposée doit fournir un accès aux applications à l'aide de WSAM (Windows Version SAM)
36. La solution souhaitée doit permet d'ajouter automatiquement de nouvelles connexions à un client VPN lorsqu'il rencontre de nouvelles passerelles prises en charge via le navigateur

Web.

37. La solution souhaitée doit permettre d'utiliser un navigateur intégré pour :
    - SAML
    - Une connexion personnalisée
    - Une authentification basée sur un jeton.
38. La solution proposée doit être capable de Désactive l'accès sans fil de l'Endpoint lorsqu'une connexion filaire est disponible.
39. Le client VPN Windows doit supporter au minimum le mode ci-après :
    - User
    - Machine
    - Machine ou User
40. La solution proposée doit disposer des mécanismes de connexion ci-après :
    - Les politiques de Sign-In : pour définir les URL d'accès à la plateforme
    - Authentification REALM : qui doit permettre de choisir le serveur d'authentification des utilisateurs, les politiques d'authentification et le rôle de mapping
    - Rôle : qui doit permettre de définir les fonctionnalités d'accès et les restrictions
    - Les politiques des ressources : qui doit permettre de définir les politiques des comportements et l'action (Deny ou permit) sur une ressource donnée
41. La solution proposée doit permettre d'affecter un utilisateur à un ou plusieurs rôles
42. La solution souhaitée doit nous permettre de paramétrer les éléments ci-après lors de la configuration des rôles :
    - Activation des fonctionnalités d'Access (Web, file, application, Telnet and SSH, Terminal Services, network, meeting, and e-mail)
    - Lier des ressources disponibles à une page de bookmarks
    - Personnalisation des paramètres (personnalisation de l'interface utilisateur)
    - Paramètres des sessions utilisateurs (session settings et options)
    - Restriction des rôles : qui doit définir les critères requis par un Device utilisateur pour qu'il soit affecté à un rôle
43. La solution proposée doit fournir des modèles de profils de ressources pour les applications tierces suivantes :
    - Hosted Java applets
    - Citrix Web Interface
    - Citrix StoreFront
    - Lotus iNotes
    - Microsoft OWA
    - Microsoft SharePoint
44. La solution souhaitée doit supporter au minimum les types d'authentification ci-après :
    - Local
    - LDAP
    - NIS
    - ACE
    - RADIUS
    - Active Directory/NT
    - Anonymous
    - SiteMinder
    - Certificate
    - SAML
    - MDM Server
45. La solution proposée doit prendre en charge les fonctionnalités suivantes d'Authentification Manager :
    - New PIN mode
    - Next-token mode

- Data Encryption Standard (DES)/Secure Dial-In (SDI) encryption
- Advanced Encryption Standard (AES) encryption
- Slave Authentication Manager support
- Name locking
- Clustering

46. La solution proposée doit disposer des quatre autres options suivantes pour attribuer des rôles :
    - Nom de Groupe
    - User attributes
    - Certificate attributes
    - Custom expressions
47. La solution souhaitée doit donner la possibilité d'utiliser les informations d'identification secondaires pour un ou plusieurs des éléments suivants :
    - L'authentification additionnelle à la solution proposée
    - Kerberos SSO pour les sites web internes protégés par Windows Authentification
    - NTLM SSO pour les sites web internes protégés par Windows Authentication (401: NTLM)
    - Authentification basique SSO pour les sites web internes dans la zone intranet (401: Basic Auth)
    - NTLM SSO pour le partage des fichiers Windows interne protégé par Windows Authentification
    - Web (Remote) SSO
    - Terminal Services SSO
48. La solution proposée doit supporter les mécanismes SSO comprennant les éléments suivants :
    - Kerberos, NTLM, and basic authentication
    - Remote form POST
    - Security Assertion Markup Language
    - eTrust SiteMinder Policy Server
49. Le Java version SAM (JSAM) de la solution souhaitée doit prendre en charge au minimum les plateformes ci-dessous :
    - Windows
    - OS X
    - Linux
    - Solaris
50. La Windows SAM (WSAN) de la solution souhaitée doit proposer au minimum les options ci-après :
    - Auto-uninstall Secure Application Manager : qui doit permettre à la solution de désinstaller automatiquement le SAM après déconnexion de l'utilisateur.
    - Prompt for username and password for intranet sites
    - Auto-upgrade Secure Application Manager
    - The user must have administrator privileges for Connect Secure to automatically install SAM on the client
    - Resolve only host names with domain suffixes in the device DNS domains
    - La solution souhaitée doit supporter au minimum les paramétrages ci-après pour les politiques des ressources :
    - Mise en cache et options de mise en cache : qui doit permettre d'utiliser les onglets Mise en cache pour rédiger des stratégies de ressources d'accès Web et spécifier les options générales de mise en cache.
    - Contrôle d'accès Java, signature de code Java et applets : qui doit permettre d'utiliser les onglets Java pour rédiger des stratégies de ressources qui contrôlent les serveurs et les ports auxquels les applets Java peuvent se connecter et pour spécifier comment la solution réécrit les applets Java.

- Réécriture sélective, proxy pass-through et réécriture des paramètres ActiveX : qui doit permettre d'utiliser les onglets Réécriture pour créer des stratégies de ressources de réécriture sélective, des stratégies de ressources de proxy pass-through et des stratégies de ressources de réécriture de paramètres ActiveX.
- POST du formulaire SSO et cookies/en-têtes SSO : qui doit permettre d'utiliser les onglets SSO pour rédiger des politiques de ressources POST de formulaire SSO distant, ainsi que des politiques de ressources d'en-tête et de cookie.
- SAML SSO et SAML Access Control : qui doit permettre d'utiliser les onglets SAML pour écrire des stratégies d'artefact et de ressources SSO Security Assertion Markup Language (SAML), des stratégies de ressources de profil SAML POST et activer les transactions de contrôle d'accès.
- Stratégies de proxy Web et serveurs proxy Web : qui doit permettre d'utiliser les onglets Proxy Web pour rédiger des stratégies de ressources de proxy Web et spécifier des serveurs proxy Web.
- Lancer JSAM : qui doit permettre d'utiliser l'onglet Lancer JSAM pour créer une stratégie de ressources Lancer JSAM.
- Options : qui doit permettre d'utiliser l'onglet Options pour spécifier les options des ressources Web.

51. La solution souhaitée doit proposer les options des sessions ci-dessous au minimum :
    - Idle Timeout : Nombre de minutes pendant lesquelles une session peut rester inactive avant d'être déconnectée.
    - Max. Session Length : Nombre de minutes pendant lesquelles une session peut rester ouverte avant d'être déconnectée.
    - Reminder Time : Nombre de minutes avant l'expiration d'une session pendant lequel les utilisateurs doivent être avertis qu'ils seront déconnectés.
    - Activer l'avertissement d'expiration de session : concerne l'heure de rappel répertoriée précédemment. Si cette option est activée, les utilisateurs doivent recevoir un avertissement du nombre de minutes spécifié avant d'être déconnectés. S'il est désactivé, les utilisateurs ne reçoivent aucun avertissement.
    - Session itinérante ou Roaming Session : qui doit fonctionner sur les adresses IP sources pour permettre aux utilisateurs mobiles disposant d'adresses IP dynamiques de se connecter à un emplacement, puis de poursuivre leur session à partir d'un autre emplacement.
    - Session persistante
    - Remove Browser Session Cookie
    - Persistent password caching
52. La solution souhaitée doit proposer les informations ci-dessous dans leurs Logs d'évènements :
    - Requêtes des Connections
    - System Status events incluant les erreuers errors et watchdog alerts
    - Rewrite events
    - System Erreurs
    - Evènement de License Protocol
    - MDM API Traces
    - Evènement des Profiler
    - Evènement de l'Accès HTML5
    - Statistiques incluant des mises à jour horaires sur le nombre d'utilisateurs connectés à l'appareil
    - Événements de performances liés à l'utilisation du processeur et de la mémoire
    - Événements de Reverse Proxy
53. Le Dashboard Cloud Secure de la solution souhaitée doit fournir des données complètes concernant l'accès aux applications Cloud dans divers graphiques :

- Top 5 Successful SSO Apps
- Top 5 Failed SSO Apps
- Devices Compliance Stats
- SSO Device details
- SSO Apps Trend
- Top 5 SSO User Roles

54. La solution souhaitée doit supporter jusqu'à 2 nœuds dans un cluster actif/passif et jusqu'à 4 nœuds dans un cluster actif/actif

Installation, Configuration et mise en œuvre

Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution, ainsi que le planning de réalisation.

Le prestataire doit accompagner l'ONDA pour l'élaboration des guides de durcissement des composants.

Ces prestations doivent inclure l'ingénierie, l'installation, la configuration, le paramétrage, l'intégration et la mise en service de la solution de sécurité proposée.

Le prestataire doit réaliser tout essai qu'il jugera nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité.

- Le titulaire assurera ainsi la mise en place de l'architecture technique cible et la mise en service des dispositifs de la solution.
- La prestation de service demandée est résumée dans les points suivants :
- Élaborer l'architecture technique de la plateforme, et l'ingénierie d'interconnexion avec l'existant.
- Assurer le transfert de compétences sur la solution.

Installation et Configuration :

- Installation, paramétrage et optimisation de la partie serveur ;
- Installation et paramétrage des agents à déployer sur les serveurs ;
- Mise en place et paramétrage de la partie gestion des droits ;
- Mise en place et paramétrage de la partie reporting ;
- Mise en place et paramétrage de la partie délégation des droits ;

Formation

Le prestataire est tenu d'assurer une session de formation au profit des équipes de l'ONDA pour une durée de 5 jours

Le soumissionnaire est tenu à présenter au niveau de l'offre technique :

- Un Engagement de renouvellement du support auprès de l'éditeur durant la période de maintenance ;
- Une attestation de l'éditeur de la solution cible proposée autorisant le soumissionnaire à répondre à cet Appel d'Offres

Livrables :

Pour chaque solution, le prestataire est tenu à livrer :

- Présentation de la solution
- Dossier d'analyse de l'existant
- Dossier d'ingénierie et d'architecture de déploiement
- Dossier d'exploitation
- Manuel d'utilisation
- Support de formation

ARTICLE 13 : CONTROLE ET VERIFICATION

L'ONDA aura le droit de contrôler et/ou d'essayer les prestations pour s'assurer qu'elles sont bien conformes au marché. L'ONDA notifiera par écrit au titulaire l'identité de ses représentants à ces fins.

Si l'une quelconque des prestations contrôlées ou essayées se révèle non conforme aux spécifications, l'ONDA la refuse. Le titulaire devra alors reprendre les prestations refusées sans aucun frais supplémentaire pour l'ONDA.

Le droit de l'ONDA de vérifier, d'essayer et, lorsque cela est nécessaire, de refuser les prestations ne sera en aucun cas limité, et l'ONDA n'y renoncera aucunement du fait que lui-même ou son représentant les aura antérieurement inspectées, essayées et acceptées.

Rien de ce qui est stipulé dans cet article ne libère le titulaire de toute obligation de garantie ou autre, à laquelle il est tenu au titre du présent marché.

ARTICLE 14 : DEFINITION DES PRIX

Les prix Les prix sont définis conformément aux dispositions de l'article 53 du CCAG-T

Prix 1 : Fourniture et mise en place d'une solution WAF :

Ce prix rémunère l'acquisition de la solution WAF avec support d'un (1) an à compter de la date de réception provisoire telle que définie dans l'article « CONSISTANCE DES PRESTATIONS » des clauses techniques de la présente tranche du marché, y compris toutes sujétions.

Prix payé au forfait au prix n°1 du Bordereau des prix-détail estimatif de la tranche ferme

Prix 2 : Fourniture et mise en place d'une solution de durcissement des configurations :

Ce prix rémunère l'acquisition de la solution de durcissement des configurations avec support d'un (1) an à compter de la date de réception provisoire telle que définie dans l'article « CONSISTANCE DES PRESTATIONS » des clauses techniques de la présente tranche du marché, y compris toutes sujétions.

Prix payé au forfait au prix n°2 du Bordereau des prix-détail estimatif de la tranche ferme

Prix 3 : Mise en place d'un Concentrateur VPN/ Traçabilité VPN :

Ce prix rémunère l'acquisition de la solution d'un Concentrateur VPN/ Traçabilité VPN avec support d'un (1) an à compter de la date de réception provisoire telle que définie dans l'article « CONSISTANCE DES PRESTATIONS » des clauses techniques de la présente tranche du marché, y compris toutes sujétions.

Prix payé au forfait au prix n°3 du Bordereau des prix-détail estimatif de la tranche ferme

Prix 4 : Mise en place d'une solution NAC :

Ce prix rémunère l'acquisition de la solution NAC avec support d'un (1) an à compter de la date de réception provisoire telle que définie dans l'article « CONSISTANCE DES PRESTATIONS » des clauses techniques de la présente tranche du marché, y compris toutes sujétions.

Prix payé au forfait au prix n°4 du Bordereau des prix-détail estimatif de la tranche ferme

CHAPITRE 3 : CLAUSES TECHNIQUES – Tranche conditionnelle-

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

N.B : Les éventuels marques commerciales, références au catalogue, appellations, brevets, conception, types, origines ou producteurs particuliers mentionnés dans les clauses techniques sont données à titre indicatif. Le cas échéant, le prestataire peut les substituer par toute autre proposition ayant des caractéristiques équivalentes et qui présentent une performance et qualité égales ou supérieures à celles qui sont exigées.

ARTICLE 01 : MAITRE D'ŒUVRE

Le maitre d'œuvre de la tranche conditionnelle du présent marché est la **Direction des Systèmes d'Information.**

ARTICLE 02 : NATURE DES PRESTATIONS ET REVISION DES PRIX

La présente tranche conditionnelle concerne des prestations de service dont les prix applicables sont fermes et non révisables.

ARTICLE 03 : DUREE DU MARCHE

La présente tranche conditionnelle du marché est valable pour une durée **d'une (1) année** à compter de la date de l'ordre de service prescrivant le commencement des prestations de cette tranche (après la réception définitive de la tranche ferme du présent marché).

Elle sera reconduite automatiquement d'année en année pour une période globale de Trois (3) ans, sauf résiliation demandée par l'une des parties trois mois à l'avance de la fin de fin de chaque année du marché (date d'anniversaire).

ARTICLE 04 : CAUTIONNEMENT DEFINITIF – RETENUE DE GARANTIE - TRANCHE CONDITIONNELLE

a) **Cautionnement** : Le cautionnement définitif est fixé à **Trois pour cent (3%)** du montant initial de la présente tranche du marché correspondant à la tranche conditionnelle arrondi au dirham supérieur conformément aux dispositions de **l'article 12 du C.C.A.G-EMO.**

b) **Retenue de garantie** : Par dérogation aux dispositions **l'article 40 du C.C.A.G-EMO,** aucune retenue de garantie ne sera opérée au titre du présent marché.

Toutes les cautions présentées sous forme de cautions personnelles et solidaires doivent contenir la mention « à première demande de l'ONDA » et être émises par un organisme marocain agréé.

ARTICLE 05 : DELAI DE GARANTIE

Par dérogation à l'article 48 du C.C.A.G-EMO et compte de la nature des travaux aucun délai de garantie n'est prévu.

ARTICLE 06 : RECEPTION DES PRESTATIONS DE TRANCHE CONDITIONNELLE

Les réceptions partielles des prestations sont autorisées

Les attestations de prestations réalisées sont signées par les responsables habilités et **seront établies trimestriellement.**

Compte tenu de la nature des prestations, la réception définitive sera prononcée conformément aux dispositions de l'article 49 du CCAG-EMO.

ARTICLE 07 : MODE DE PAIEMENT

L'ONDA se libérera des sommes dues en exécution de la tranche conditionnelle du présent marché en faisant donner crédit au compte ouvert au nom du prestataire indiqué sur l'acte d'engagement.

Les paiements partiels seront effectués trimestriellement à terme échu.

Le paiement des sommes dues est effectué, dans un délai maximum de quatre-vingt-dix jours (90) à compter de la date de réception des prestations demandées et sur présentation de factures en cinq exemplaires.

Dispositions relatives à la facturation :

- Les factures doivent être émises au plus tard le dernier jour du mois de la réalisation des prestations objet du présent marché.
- Les factures doivent se conformer aux dispositions règlementaires notamment les articles 145 alinéa III et 146 du Code Général des Impôts Marocain en vigueur.
- Les factures doivent porter les dates de leur établissement.
- En cas de remise tardive de la facture générant ainsi une sanction pécuniaire, au profit du Trésor, à l'encontre de l'ONDA, le montant de ladite sanction pécuniaire sera déduit, le cas échéant, à l'identique des sommes dues au prestataire.

ARTICLE 08 : PENALITES POUR RETARD

A défaut par le titulaire d'avoir terminé les prestations définies par le présent marché ou d'avoir respecté tout planning ou délai prévue par ce marché, il lui sera appliqué sans préjudice de l'application des mesures prévues à l'article 42 du CCAG EMO, une pénalité de **cinq pour mille (5‰)** du montant initial du marché, éventuellement modifié ou complété par les avenants intervenus, par jour de retard.

La pénalité est plafonnée à **dix pour cent (10%)** du montant initial du marché, éventuellement modifié ou complété par les avenants intervenus ; au-delà de ce plafond, l'O.N.D.A. se réserve le droit de procéder à la résiliation du marché sans préjudice des mesures correctives prévues par l'article 52 du CCAG EMO.

Les sommes concernant les pénalités seront déduites des décomptes de l'entreprise sans qu'il ne soit nécessaire d'une mise en demeure préalable.

ARTICLE 09 : BREVETS

L'entrepreneur garantira le maître d'ouvrage contre toute réclamation des tiers relative à la contrefaçon ou à l'exploitation non autorisée d'une marque commerciale ou de droit de création industrielle résultant de l'emploi des fournitures ou d'un de leurs éléments.

ARTICLE 10 : NORMES

Les fournitures livrées en exécution de la présente tranche du marché doivent être conformes aux normes Marocaines ou autres normes applicables au Maroc en vertu d'accords internationaux fixées aux prescriptions et spécifications techniques du présent marché ou à des normes internationales en cas d'absence desdites normes.

ARTICLE 11 : GARANTIE PARTICULIERE

Le Prestataire garantit que toutes les fournitures éventuellement livrées en exécution de la présente tranche du marché sont neuves, n'ont jamais été utilisées, sont du modèle le plus récent en service et incluent toutes les dernières améliorations en matière de conception et

de matériaux, sauf si le marché en a disposé autrement. Le titulaire garantit en outre que les fournitures livrées en exécution du marché n'auront aucune défectuosité due à leur conception, aux matériaux utilisés ou à leur mise en œuvre (sauf dans la mesure où la conception ou le matériau est requis par les spécifications de l'ONDA) ou à tout acte ou omission du titulaire, survenant pendant l'utilisation normale des fournitures livrées dans les conditions prévalant dans le pays de destination finale.

ARTICLE 12 : DESCRIPTION TECHNIQUE DES PRESTATIONS

Pour chaque solution et après déclenchement de la tranche conditionnelle, le prestataire est tenu de fournir le support annuel pour les solutions installées.

le prestataire est tenu de réaliser quatre (04) visites de maintenance préventive annuelle sur les lieux d'installation des équipements objet de ce cahier des charges (à raison d'une visite par trimestre).

Le prestataire est tenu de fournir un planning de visites annuel qui doit être communiqué au responsable ONDA le premier moi de chaque année.

Opérations à réaliser :

A chaque visite, le prestataire est tenu de mener les opérations nécessaires pour assurer un bon niveau technologique du système à savoir :

- Test et contrôle des différents équipements ;
- Installation des mises à jour logicielles des différents composants de la solution. il s'agit de garantir la mise à niveau du parc logiciel et/ou matériel objet de la maintenance ;
- L'entretien du matériel et du logiciel ;
- La réparation ou le remplacement total ou partiel des pièces défectueuses ;
- La correction de tout « bug » détecté au niveau du logiciel (y compris l'installation des patchs correctifs ou préventifs) ;
- La livraison et l'installation des nouvelles versions logicielles. Le parc logiciel objet de la maintenance doit être à niveau avec la dernière version stable et validée ;

Aussi, la maintenance préventive comprend-t-elle le nettoyage du matériel, les tests, les mises au point nécessaires, le remplacement des pièces défectueuses ou obsolètes.

Le planning de maintenance doit tracer à l'avance les actions préventives à mener chaque année (Upgrade, patching, mise à niveau matériel, …).

A signaler que les pièces de rechange et les produits de nettoyage des différentes composantes à entretenir sont à la charge du prestataire.

Le prestataire est tenu de fournir pour chaque mise à jour majeure des logiciels objets du présent CPS les média (CD-ROM/DVD/mémoire …) d'installation.

Il y a lieu de signaler que les actions de maintenance préventives doivent être validées et approuvées par ONDA avant de leur mise en place.

Rapport de la maintenance préventive :

A l'issue de chaque visite de maintenance, le prestataire est tenu de présenter au responsable concerné de ONDA un rapport détaillé de la maintenance.

Le rapport doit détailler ce qui suit :

- Les actions de maintenance réalisées ;
- Les recommandations en termes d'amélioration d'architecture ou autre ;
- Les actions prévues lors de la prochaine visite préventive ;
- Les incidents survenus sur le trimestre en cours ;
- Tous risques ou alertes à signaler afin d'éviter toute complication par la suite ;

Planning des visites :

Le prestataire est tenu de fournir, au moment de la notification et après chaque reconduction du contrat de maintenance, un planning prévisionnel des visites le premier moi de chaque année.

Vielle sécurité :

Le prestataire est tenu d'aviser et alerter ONDA de tous les risques, alertes, vulnérabilités ou menaces liés aux équipements et logiciels objet de la maintenance.

Maintenance Sur Demande :

Le prestataire est tenu d'intervenir sur demande et après chaque signalisation d'un incident, qui inclut la remise en bon état de fonctionnement du matériel par le remplacement des pièces défectueuses, la reconfiguration d'un composant logiciel ou la réinstallation d'un système. Les pièces de rechange sont à la charge du prestataire.

Le prestataire est tenu de présenter au responsable concerné de ONDA un rapport détaillé de l'intervention.

Niveau de service

Le prestataire est tenu d'assurer le niveau de service suivant :

- Astreinte : Horaires normales ;
- Délai maximal d'intervention : 4 heures après déclaration de l'incident ;
- Délai maximal de réparation : 8 heures après déclaration de l'incident ;

Le prestataire est tenu de communiquer à ONDA les coordonnées des personnes / services à contacter en cas d'un incident (durant et hors les heures de service).

Toute intervention ou réparation dépassant les délais suscités sera soumise à une pénalité de retard de 1%0 (Pour mille) pour chaque heure dépassée.

Liste de la permanence :

Le prestataire est tenu de fournir une liste des personnes en astreinte à contacter en cas d'incident survenu hors les heures de service, les week-ends et/ou les jours fériés. Une procédure d'escalade doit être prévue en cas d'indisponibilité des personnes concernées par l'astreinte.

Rapport d'intervention :

Le prestataire est tenu de fournir un rapport d'intervention après chaque résolution d'incident.

Le rapport doit être soumis à la validation du responsable ONDA concerné.

Interlocuteur unique :

Le prestataire est tenu de désigner un responsable du compte comme interlocuteur unique pour gérer tous les aspects liés à la maintenance (planification, non réponse de la liste d'astreinte, dépassement des délais contractuels, …).

Lieu de la maintenance : Siège ONDA

ARTICLE 13 : CONTROLE ET VERIFICATION

L'ONDA aura le droit de contrôler et/ou d'essayer les fournitures pour s'assurer qu'elles sont bien conformes au marché. L'ONDA notifiera par écrit au titulaire l'identité de ses représentants à ces fins.

Si l'une quelconque des fournitures contrôlées ou essayées se révèle non conforme aux spécifications, l'ONDA la refuse; Le titulaire devra alors remplacer les fournitures refusées sans aucun frais supplémentaire pour l'ONDA.

Le droit de l'ONDA de vérifier, d'essayer et, lorsque cela est nécessaire, de refuser les fournitures ne sera en aucun cas limité, et l'ONDA n'y renoncera aucunement du fait que lui-même ou son représentant les aura antérieurement inspectées, essayées et acceptées.

Rien de ce qui est stipulé dans cet article ne libère le titulaire de toute obligation de garantie ou autre, à laquelle il est tenu au titre du présent marché.

ARTICLE 14 : DEFINITION DES PRIX

Les prix Les prix sont définis conformément aux dispositions de l'article 34 du CCAG-EMO

Appel d'offres ouvert N° 088-24-AOO

Fourniture, déploiement et maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche ferme : Fourniture et déploiement des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information

Tranche conditionnelle : Maintenance des solutions pour le renforcement de la résilience cybersécurité des Systèmes d'Information